Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983 – 2013

International Documents on Data Protection in Telecommunications and Media 1983 – 2013

Impressum

Herausgeber: **Berliner Beauftragter für Datenschutz und Informationsfreiheit**
An der Urania 4 – 10
10787 Berlin
Telefon: 0 30/1 38 89-0
Telefax: 0 30/2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Druck: LASERLINE Digitales Druckzentrum
Bucec & Co. Berlin KG

Inhaltsverzeichnis / Contents

Einleitung

Seit der letzten Veröffentlichung der internationalen Dokumente zum Datenschutz bei Telekommunikation und Medien 2006 hat sich die Welt grundlegend verändert. Die von Edward Snowden im Sommer 2013 ausgelösten Veröffentlichungen über die unkontrollierte und maßlose Überwachung der weltweiten Telekommunikation durch die US National Security Agency und andere Nachrichtendienste hat die Vollversammlung der Vereinten Nationen veranlasst, im Dezember 2013 eine Resolution zur Bedeutung des „Rechts auf Privatheit im digitalen Zeitalter" zu verabschieden. Mit dieser Resolution beginnt die hier vorgelegte aktualisierte Dokumentensammlung, die den Zeitraum von 1983 bis 2013 umfasst.

In dieser Zeit hat die vom Berliner Beauftragten für Datenschutz* schon 1980 ins Leben gerufene Internationale Arbeitsgruppe zum Datenschutz bei Telekommunikation und Medien (weltweit auch als „Berlin Group" bekannt), bestehend aus Vertretern von Datenschutzbehörden und Experten aus aller Welt, eine Vielzahl datenschutzrechtlicher Themen diskutiert und hierzu Stellungnahmen und Empfehlungen beschlossen. Dabei hat sie sehr frühzeitig auf technische Neuerungen und die damit verbundenen Risiken für den Schutz der Privatsphäre aufmerksam gemacht und Konzepte entwickelt, wie man diese Risiken beherrschen könnte.

Schon das „Budapest-Berlin-Memorandum" vom April 1996 weist auf die grundsätzliche Bedeutung des Fernmeldegeheimnisses für die weltweite Kommunikation hin und fordert dessen Schutz durch nationale Gesetze und internationale Abkommen. Zugleich hat sich die Arbeitsgruppe für die Nutzung von sicheren Verschlüsselungsmethoden eingesetzt. Diese Forderungen wurden in mehreren späteren Arbeitspapieren, zuletzt – unter dem Eindruck der exzessiven Praktiken verschiedener Nachrichtendienste – im September 2013 präzisiert. De Internationale Konferenz der Datenschutzbeauftragten hat sie wenig später aufgegriffen. Ähnliche Aufrufe zum Handeln enthält auch die erwähnte Resolution der UN-Vollversammlung vom Dezember 2013.

Es bleibt zu hoffen, dass damit ein Prozess begonnen hat, der möglichst bald in verbindliche und überprüfbare internationale Garantien für den Schutz der Privatsphäre und der vertraulichen Kommunikation mündet.

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit
Vorsitzender der Arbeitsgruppe

* Dr. Hans-Joachim Kerkau. Von 1990 bis 2005 war Prof. Dr. Hansjürgen Garstka Vorsitzender der Internationalen Arbeitsgruppe.

Introduction

Since the last collection of International Documents on Data Protection in Telecommunications and Media was published in 2006 the world has changed fundamentally. The publication of documents – initiated by Edward Snowden – on the unchecked and excessive surveillance of worldwide telecommunications by the US National Security Agency and other intelligence agencies has led in December 2013 to the adoption by the UN General Assembly of a resolution on the "The Right to Privacy in the Digital Age". This resolution is the first document in this updated collection of documents on data protection in telecommunications and media covering the period from 1983 to 2013.

During this period the International Working Group on Data protection in Telecommunications (internationally also known as the "Berlin Group") which had been initiated by the Berlin Commissioner for Data Protection* in 1980 and which consists of representatives of data protection authorities as well as experts from all over the world has discussed a great number of data protection and privacy issues and adopted working papers and recommendations. Very early the Working Group has identified technical developments and related risks to privacy and has made recommendations how to tackle these risks.

Already the "Budapest-Berlin-Memorandum" of April 1996 highlights the fundamental importance of the secrecy of telecommunications for global correspondence and calls for the protection of this secrecy by national legislation and international agreements. At the same time the Working Group has called for the use of secure encryption technology. These recommendations were later elaborated on numerous occasions, most recently in September 2013 – under the impression of excessive surveillance by several intelligence agencies. They were taken up by the International Conference of Data Protection Commissioners soon afterwards. The abovementioned resolution of the UN General Assembly of December 2013 contains similar calls for action.

It is to be hoped that this has started a development leading as soon as possible to binding and effective international guarantees for the protection of privacy and secrecy of telecommunications.

Dr. Alexander Dix
Berlin Commissioner for Data Protection and Freedom of Information
Chairman of the Working Group

* Dr. Hans-Joachim Kerkau. From 1990 to 2005 the Working Group was chaired by Prof. Dr. Hansjürgen Garstka.

A. Resolution der UN-Vollversammlung vom 18. Dezember 2013 / Resolution adopted by the General Assembly on 18 December 2013 (A/RES/68/167)

Das Recht auf Privatheit im digitalen Zeitalter

Die Generalversammlung,

in Bekräftigung der Ziele und Grundsätze der Charta der Vereinten Nationen,

sowie in Bekräftigung der in der Allgemeinen Erklärung der Menschenrechte und den einschlägigen internationalen Menschenrechtsverträgen, einschließlich des Internationalen Paktes über bürgerliche und politische Rechte und des Internationalen Paktes über wirtschaftliche, soziale und kulturelle Rechte, verankerten Menschenrechte und Grundfreiheiten,

ferner in Bekräftigung der Erklärung und des Aktionsprogramms von Wien,

feststellend, dass das rasche Tempo der technologischen Entwicklung Menschen in der ganzen Welt in die Lage versetzt, sich neuer Informations- und Kommunikationstechnologien zu bedienen, und gleichzeitig die Fähigkeit der Regierungen, Unternehmen und Personen zum Überwachen, Abfangen und Sammeln von Daten vergrößert, das eine Verletzung oder einen Missbrauch der Menschenrechte darstellen kann, insbesondere des in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und in Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte festgelegten Rechts auf Privatheit, weshalb diese Frage in zunehmendem Maße Anlass zur Sorge gibt,

in Bekräftigung des Menschenrechts auf Privatheit, dem zufolge niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr ausgesetzt werden darf, und des Anspruchs auf rechtlichen Schutz gegen solche Eingriffe sowie in der Erkenntnis, dass die Ausübung des Rechts auf Privatheit für die Verwirklichung des Rechts auf freie Meinungsäußerung und auf unbehinderte Meinungsfreiheit wichtig ist und eine der Grundlagen einer demokratischen Gesellschaft bildet,

unter nachdrücklichem Hinweis auf die Wichtigkeit der uneingeschränkten Achtung der Freiheit, Informationen sich zu beschaffen, zu empfangen und weiterzu-

geben, namentlich auch die grundlegende Wichtigkeit des Zugangs zu Informationen und der demokratischen Teilhabe,

unter Begrüßung des dem Menschenrechtsrat auf seiner dreiundzwanzigsten Tagung vorgelegten Berichts des Sonderberichterstatters über die Förderung und den Schutz der Meinungsfreiheit und des Rechts der freien Meinungsäußerung[1] zu den Auswirkungen, die das Überwachen von Kommunikation durch die Staaten auf die Ausübung der Menschenrechte auf Privatheit und auf Meinungsfreiheit und freie Meinungsäußerung hat,

betonend, dass das rechtswidrige oder willkürliche Überwachen und/oder Abfangen von Kommunikation sowie die rechtswidrige oder willkürliche Sammlung personenbezogener Daten, als weitreichende Eingriffe, die Rechte auf Privatheit und freie Meinungsäußerung verletzen und im Widerspruch zu den Prinzipien einer demokratischen Gesellschaft stehen können,

feststellend, dass Besorgnisse über die öffentliche Sicherheit das Sammeln und den Schutz bestimmter sensibler Informationen zwar rechtfertigen können, dass die Staaten jedoch die vollständige Einhaltung ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen sicherstellen müssen,

tief besorgt über die nachteiligen Auswirkungen, die das Überwachen und/oder Abfangen von Kommunikation, einschließlich des extraterritorialen Überwachens und/oder Abfangens von Kommunikation, sowie die Sammlung personenbezogener Daten, insbesondere wenn sie in massivem Umfang durchgeführt werden, auf die Ausübung und den Genuss der Menschenrechte haben können,

bekräftigend, dass die Staaten sicherstellen müssen, dass alle zur Bekämpfung des Terrorismus ergriffenen Maßnahmen mit ihren Verpflichtungen nach dem Völkerrecht, insbesondere den internationalen Menschenrechtsnormen, dem Flüchtlingsvölkerrecht und dem humanitären Völkerrecht, im Einklang stehen,

1. *bekräftigt* das Recht auf Privatheit, dem zufolge niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr ausgesetzt werden darf, und den Anspruch auf rechtlichen Schutz gegen solche Eingriffe, wie in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und in Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte festgelegt;

2. *ist sich dessen bewusst*, dass der globale und offene Charakter des Internets und das rasche Voranschreiten der Informations- und Kommunikationstechno-

[1] A/HRC/23/40 und Corr.1.

logien als eine treibende Kraft für die Beschleunigung des Fortschritts bei der Entwicklung in ihren verschiedenen Formen wirken;

3. *erklärt*, dass die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen, einschließlich des Rechts auf Privatheit;

4. *fordert* alle Staaten *auf*:

   a) das Recht auf Privatheit zu achten und zu schützen, namentlich im Kontext der digitalen Kommunikation;

   b) Maßnahmen zu ergreifen, um Verletzungen dieser Rechte ein Ende zu setzen und die Bedingungen dafür zu schaffen, derartige Verletzungen zu verhindern, namentlich indem sie sicherstellen, dass die einschlägigen innerstaatlichen Rechtsvorschriften mit ihren Verpflichtungen nach den internationalen Menschenrechtsnormen im Einklang stehen;

   c) ihre Verfahren, Praktiken und Rechtsvorschriften hinsichtlich der Überwachung von Kommunikation, deren Abfangen und der Sammlung personenbezogener Daten zu überprüfen, namentlich Überwachen, Abfangen und Sammeln in massivem Umfang, mit dem Ziel, das Recht auf Privatheit zu wahren, indem sie die vollständige und wirksame Umsetzung aller ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen sicherstellen;

   d) unabhängige, wirksame innerstaatliche Aufsichtsmechanismen einzurichten oder bestehende derartige Mechanismen beizubehalten, die in der Lage sind, Transparenz, soweit angebracht, und Rechenschaftspflicht der staatlichen Überwachung von Kommunikation, deren Abfangen und der Sammlung personenbezogener Daten sicherzustellen;

5. *ersucht* die Hohe Kommissarin der Vereinten Nationen für Menschenrechte, dem Menschenrechtsrat auf seiner siebenundzwanzigsten Tagung und der Generalversammlung auf ihrer neunundsechzigsten Tagung einen Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen zur Prüfung durch die Mitgliedstaaten vorzulegen;

6. *beschließt*, diese Frage auf ihrer neunundsechzigsten Tagung unter dem Unterpunkt „Menschenrechtsfragen, einschließlich anderer Ansätze zur besseren Gewährleistung der effektiven Ausübung der Menschenrechte und Grundfreiheiten“ des Punktes „Förderung und Schutz der Menschenrechte“ zu behandeln.

The right to privacy in the digital age

The General Assembly,

Reaffirming the purposes and principles of the Charter of the United Nations,

Reaffirming also the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights[1] and relevant international human rights treaties, including the International Covenant on Civil and Political Rights[2] and the International Covenant on Economic, Social and Cultural Rights,[2]

Reaffirming further the Vienna Declaration and Programme of Action,[3]

Noting that the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,

Reaffirming the human right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, and recognizing that the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society,

Stressing the importance of the full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation,

Welcoming the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,[4] submitted to the Human Rights Council at its twenty-third session, on the implications of State surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression,

---

[1] Resolution 217 A (III).

[2] See resolution 2200 A (XXI), annex.

[3] A/CONF.157/24 (Part I), chap. III.

[4] A/HRC/23/40 and Corr.1.

Emphasizing that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society,

Noting that while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights,

Reaffirming that States must ensure that any measures taken to combat terrorism are in compliance with their obligations under international law, in particular international human rights, refugee and humanitarian law,

1. *Reaffirms* the right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights[1] and article 17 of the International Covenant on Civil and Political Rights;[2]

2. *Recognizes* the global and open nature of the Internet and the rapid advancement in information and communications technologies as a driving force in accelerating progress towards development in its various forms;

3. *Affirms* that the same rights that people have offline must also be protected online, including the right to privacy;

4. *Calls upon* all States:

   (a) To respect and protect the right to privacy, including in the context of digital communication;

   (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

   (c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal

data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data;

5. *Requests* the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States;

6. *Decides* to examine the question at its sixty-ninth session, under the sub-item entitled "Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms" of the item entitled "Promotion and protection of human rights".

70th plenary meeting
18 December 2013

B. Beschlüsse der Internationalen Konferenz der Datenschutzbeauftragten / Resolutions of the International Conference of Data Protection Commissioners

1983

5. Konferenz, 18. Oktober 1983, Stockholm

Neue Medien

Die Internationale Konferenz der Datenschutzbeauftragten geht übereinstimmend davon aus, daß der Einsatz Neuer Medien, die über Kabelnetze verbreitet werden, eine erhebliche Gefährdung für die Persönlichkeitsrechte mit sich bringen kann.

Soweit bei den Neuen Medien die Kommunikation zwischen Informationsanbietern und Teilnehmern durch elektronische Datenverarbeitungsanlagen gesteuert wird, ist – im Gegensatz zu herkömmlichen Medien – die Speicherung personenbezogener Daten in einem gewissen Umfang erforderlich.

So werden beim Medium „Bildschirmtext“ (Videotext) Verbindungs- und Abrechnungsdaten gespeichert. Bei manchen Diensten werden die vom Teilnehmer abgerufenen Sendungen registriert. Das Recht der Unverletzlichkeit der Wohnung wird berührt, wenn mit neuen Diensten von außen in den Wohnungen Wirkungen ausgelöst und Messungen vorgenommen werden.

Über die auf diese Weise an zentralen Stellen automatisiert entstehenden Sammlungen personenbezogener Daten könnten Persönlichkeitsprofile aller Benutzer erstellt werden. Deren soziale Beziehungen und Verhaltensweisen können damit zum Gegenstand von Maßnahmen gemacht werden.

Darüber hinaus können mit Hilfe der neuen Medien personenbezogener Daten jeglicher Art mit geringem Aufwand und in großem Umfang verbreitet werden. Erfahrungen mit Bildschirmtext haben gezeigt, daß Anbieter und Benutzer mißbräuchlich sensible Daten über die Neuen Medien veröffentlichen.

5th Conference, 18th October 1983, Stockholm

New Media

There was consensus at the International Conference of Data Protection Commissioners that the application of the new media, which will be circulated by cable

networks, might well be accompanied by considerable danger to the individual's rights to privacy.

As far as communication between information providers and subscribers is controlled by electronic data processing systems, a certain amount of personal data needs to be stored, which is not the case with traditional media.

Videotext is a good example of this where call and accounting data are stored. Some services register transmissions called up by subscribers. The right to inviolability of an individual's privacy at home is infringed upon if the new services are able to induce effects in the home from any remote location and whenever measurements are made.

Personal data which automatically collected at central places in this manner can be used to draw up individual profiles of all users. Users' social relations and patterns of behaviour can in this way be made object of other measures.

In addition to the above, the new media can be used to circulate at little expense copious quantities of all kinds of private data. Experience with videotex has indicated that providers and users misuse sensitive data making it public over the new media.

1985

7. Konferenz, 26. September 1985, Luxemburg

Datenschutz und Neue Medien

1. Die Internationale Konferenz der Datenschutzbeauftragten hat am 18. Oktober 1983 auf ihrer Sitzung in Stockholm einen Beschluß zum Thema Neue Medien gefaßt, in dem gefordert wurde, daß durch geeignete Maßnahmen, insbesondere der Gesetzgebung, in jedem Land die Betriebsbedingungen so gestaltet werden, daß durch den Einsatz der Neuen Medien Persönlichkeitsrechte nicht beeinträchtigt werden.

2. Die Weiterentwicklung der Neuen Medien in den einzelnen Staaten bestätigt einerseits die Notwendigkeit der Forderungen, zeigt aber andererseits auch zusätzliche Gefährdungen auf.

   – Die internationale Standardisierung der Telekommunikationsdienste und die zunehmende grenzüberschreitende Vernetzung der Systeme machen interna-

tionale Vereinbarungen auch über den Datenschutz bei neuen Informations- und Kommunikationsdiensten dringlich.

– Der beginnende Aufbau von Glasfasernetzen, die anstehende Einführung der Breitbandkommunikation und die Integration der einzelnen Telekommunikationsdienste, verbunden mit der Digitalisierung von schmal- und breitbandigen Übertragungsnetzen werden zu einer erheblichen Zunahme der Informationsströme führen. Gleichzeitig werden Integration und Digitalisierung zu einer besseren Auswertbarkeit mit Hilfe automatischer Anlagen führen und damit die Gefahr des unbefugten Aufzeichnens und Auswertens der übermittelten Informationen erhöhen.

– Der Einsatz von Satelliten zur Kommunikation schafft im Hinblick auf die Datenintegrität und den Schutz von unbefugtem Abhören ebenfalls Risiken.

3. Die anläßlich des Erfahrungsaustausches versammelten Vertreter der nationalen Datenschutzinstitutionen appellieren daher an die internationale Konferenz der Datenschutzbeauftragten, den in ihrem Beschluß vom 18. Oktober 1983 enthaltenen Forderungen gegenüber den nationalen Regierungen Nachdruck zu verleihen und auf eine Verstärkung der internationalen Zusammenarbeit bei der Überwachung Neuer Medien hinzuwirken.

7th Conference, 26th September 1985, Luxembourg

Data Protection and New Media

1. At its meeting in Stockholm on 18th October 1983, the International Conference of Data Protection Commissioners passed a resolution on the subject of the new media. This resolution demands that suitable measures, in particular, legislation, be taken in each country to ensure that operating conditions be organised in such a way that the application of the new media in no way encroaches upon the individual's rights to privacy.

2. The further development of the new media in individual countries confirms the need for such demands; it also indicates additional dangers, however:

– International standardisation of telecommunications services and increasing transnational networking of systems make international agreements on data protection, too, with regard to new information and communication services a matter of utmost urgency.

– The beginning construction of optical fibre networks, the imminent introduction of broadband communication, and the integration of individual telecom-

munication services in conjunction with the digitalisation of narrow- and broadband transmission networks will lead to a considerable increase in information streams. At the same time, integration and digitalisation will lead to an improved ability to evaluate with the help of automatic systems. This will be accompanied by the increased danger of unauthorised recording and evaluating of transmitted information.

– The use of satellites for communication likewise induces risks with regard to data integrity and protection against unauthorised monitoring.

3. The representatives of the national data protection organisations, convened to exchange experience, therefore appeal to the International Conference of Data Protection Commissioners to draw the attention of national governments to the demands contained in their resolution of 18 October 1983, and to do all in their power to increase international cooperation in monitoring the new media.

1987

9. Konferenz, 24. September 1987, Oslo

Neue Medien

1. Die Internationale Konferenz der Datenschutzbeauftragten beobachtet seit Jahren die Entwicklung der Neuen Medien und die damit verbundenen Probleme des Datenschutzes. Sie hat mit ihren Entschließungen vom 18. Oktober 1983 in Stockholm und vom 26. September 1985 in Luxemburg Forderungen zur Verbesserung des Datenschutzes erhoben.

2. Der Stand der Massenmedien und Telekommunikation im Jahre 1987 ist durch folgende Merkmale gekennzeichnet:

   – Die verschiedenen für die Telekommunikation genutzten analogen und digitalen Einzelnetze streben nach einer Vereinheitlichung der technischen Normen; zunehmend entstehen einheitliche nationale Infrastrukturen für die Telekommunikationsnetze.

   – Dienste für die Verbreitung von Massenmedien und für andere Telekommunikationsformen verschiedenster Art werden auf diesen Netzen national und international angeboten.

3. Die Internationale Konferenz der Datenschutzbeauftragten ist besorgt über die Sammlung einer zunehmend größeren Anzahl von personenbezogenen Daten durch Massenmedien und Telekommunikationsdienst. Die Risiken sind offensichtlich, die in einer derartigen Kumulation von Daten und deren möglichen Gebrauch zu Zwecken liegen, die nicht mit den Zwecken übereinstimmen, für die sie erhoben wurden. Soweit keine anonymen Nutzungsformen eingeführt werden, ermöglicht die über die ursprünglichen Kommunikationszwecke hinausgehende Verarbeitung derartiger Informationen den Aufbau von Daten über die Lebensführung und Interessen von Einzelindividuen und Familien. Eine solche Entwicklung wird als keineswegs wünschenswert angesehen.

   Die Informationen konzentrieren sich letztlich bei wenigen öffentlichen und privaten Netzbetreibern und Kommunikationsanbietern (Post, Teleports, internationale Serviceunternehmen). Die Risiken des Mißbrauchs, der Sabotage und Spionage sowie der Manipulation bürden diesen Institutionen eine erhebliche Verantwortung auf, ohne daß in den meisten Ländern die nationalen Gesetze hinreichende rechtliche Regelungen hierfür vorsehen.

4. Die Internationale Konferenz der Datenschutzbeauftragten fordert deshalb nachdrücklich die Entwicklung von Regelungswerken auf nationaler und internationaler Ebene. Für die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung sind internationale Normen anzustreben. Die Zusammenarbeit der nationalen Kontrollinstanzen ist zu verbessern.

9th Conference, 24th September 1987, Oslo

New Media

1. For several years the International Conference of Data Protection Commissioners have been following the development of the New Media and the data protection problems it entails. In its resolutions of 18 October 1983 in Stockholm and of 26th September 1985 in Luxembourg it raised demands for the improvement of data protection in this connection.

2. The state of mass media and telecommunications in 1987 is marked by the following features:

   – The various analogous and digital individual networks used for telecommunications tend towards uniformity of technical standards; there is an trend towards national telecommunication network infrastructures.

   – The services of the mass media and other forms of telecommunication services of different kinds are offered nationally and internationally by these networks.

3. The International Conference of Data Protection Commissioners is concerned about the collection of an inscreasingly greater quantity of personalized data by the mass media and telecommunication services. The risks inherent in such an accumulation of data and its potential use for purposes other than those for which the data were obtained are obvious. Unless anonymous procedures for the use of such services will be introduced, the processing of such information beyond its original purposes could enable the building up of files of life styles and interests of individuals and families. Such a development is considered entirely undesirable.

   Informations is ultimately concentrated within the control of a few public and private network operators and providers of communication services (the postal administration, teleports, international service providers). The risks of abuse, sabotage and espionage, etc., as well as manipulation, constitute a considerable burden of responsibility for these institutions without there being national legislation containing sufficient legal provisions in most countries.

4. The International Conference of Data Protection Commissioners, therefore, emphatically demands the development of regulatory systems on a national and international level. International standards should be sought for the technical and organisational measures required to provide data protection. Cooperation between national control institutions should be further improved.

1989

11. Konferenz, 30. August 1989, Berlin

Berliner Resolution

Die Telekommunikation befindet sich weltweit in einer raschen Entwicklung. Über internationale Datennetze werden in wachsendem Umfang auch personenbezogene Daten transferiert, etwa im Zusammenhang mit der Verwendung von Kreditkarten, bei Reise-Buchungs- Systemen und innerhalb multinationaler Unternehmen. Die Nutzung dieser Technologie kann bedeutende Vorteile mit sich bringen. Aber zugleich wird es schwieriger, die Rechte derer zu schützen, deren persönliche Daten rund um die Welt übermittelt werden.

Der Europarat, die OECD, die Vereinten Nationen und weitere internationale Organisationen haben Empfehlungen und Leitlinien zum Datenschutz verabschiedet. Sie enthalten einen gemeinsamen Bestand von Grundsätzen für eine faire Praxis, wie sie etwa in der Konvention des Europarats (Konvention Nr. 108) und

in den OECD-Leitlinien zum Ausdruck kommen. Sie bezwecken den Schutz der Privatheit des einzelnen.

Bisher haben sich acht Staaten durch Beitritt zur Konvention des Europarats international verpflichtet, einen bestimmten Datenschutzstandard einzuhalten. Die Datenschutz-Kontrollinstanzen dieser Länder haben in gewissem Umfang die Befugnis, den grenzüberschreitenden Datenfluß zu kontrollieren, wenn dies zum Schutz einzelner nötig ist. Bei dieser Kontrolle ergeben sich allerdings schwerwiegende praktische Probleme. Datenübermittlung ins Ausland bedeutet deshalb für den einzelnen in der Mehrzahl der Fälle, daß er nicht mehr die Gewißheit haben kann, daß die Grundsätze, die in nationalen Gesetzen und in den verschiedenen internationalen Übereinkommen festgelegt sind, auf seine oder ihre Daten angewandt werden. Zum Beispiel kann es dann keine Garantie geben, daß die Daten auf dem neuesten Stand und genau sind und nur für bestimmte Zwecke verwendet werden. Der einzelne kann auch sein Recht, einen Datenschutzbeauftragten anzurufen, nicht wahrnehmen.

Das Problem eines wirksamen internationalen Datenschutzes läßt sich nur durch gleichwertige gesetzliche Sicherungen in den übermittelnden und empfangenden Ländern lösen. Diese Lösung wird auch von den oben genannten Empfehlungen und Leitlinien vorgezeichnet.

Nach Auffassung der Datenschutzbeauftragten muß bei der Entwicklung und Nutzung internationaler Datendienste dem Datenschutz die gleiche Priorität gegeben werden wie der Förderung der Datenverarbeitung und der Telekommunikation. Sie empfehlen deshalb:

– Die Regierungen sollten sowohl einzeln als auch im Rahmen internationaler Organisationen darauf hinarbeiten, daß so bald wie möglich gleichwertige gesetzliche Sicherungen geschaffen werden.

– Wer personenbezogene Daten über die Grenzen vermittelt, muß den Schutz beim Empfänger prüfen, daß die Beachtung der Rechte der Betroffenen tatsächlich sichergestellt wird.

Das Ziel dieser Maßnahmen muß sein:

– Die Datenschutzgrundsätze der Konvention Nr. 108 und der OECD-Leitlinien werden unabhängig von einer grenzüberschreitenden Übermittlung gewährleistet;

– International operierende Datenverarbeitungssysteme müssen so aufgebaut sein, daß der Einzelne ohne unzumutbare Schwierigkeiten seine Datenschutzrechte wahrnehmen kann;

– Berichtigungen, Aktualisierungen und Löschungen von Daten müssen auch im Ausland nachvollzogen werden, wenn die Daten zuvor dorthin übermittelt worden sind;

– Die durch den internationalen Datenaustausch erhöhten Gefahren für das Recht des einzelnen, über die Verwendung ihrer Daten zu bestimmen, müssen durch internationale Zusammenarbeit der Datenschutzbeauftragten ausgeglichen werden.

11th Conference, 30th August 1989, Berlin

Berlin Resolution

World-wide telecommunications are evolving rapidly. International data networks are increasingly used for transfers of personal data, for instance in the use of credit cards, for the purposes of travel booking systems and within multinational enterprises. The use of this new technology can bring significant benefits. But it also increases the problem of safeguarding the position of those individuals whose details are transmitted around the world.

The Council of Europe, the OECD, the United Nations and other international organisations have adopted recommendations and guidelines on data protection. A common feature is a set of principles of good practice such as those in the Council of Europe Convention (Treaty 108) and in the OECD guidelines. These good practices are designed to safeguard the privacy of individuals.

So far, eight states have acceded to the Council of Europe Convention and so committed themselves internationally to legally established data protection standards. Data protection authorities in those countries have some authority to control the transborder flow of personal data when this is necessary to protect individuals. However, controlling transborder data flows in this way presents severe practical problems. In most cases, therefore, data transmission across national borders implies that the individual can no longer ensure that the principles laid down by national laws and the various international agreements will be applied to his or her data.

For example there can be no guarantee that the data are up to date, accurate, and used only for proper purposes; and the individual loses the opportunity to appeal to any data protection commissioner.

The solution to giving effective international protection to personal data lies in equivalent legal safeguards in the transmitting and receiving countries. This solu-

tion is consistent with the international recommendations and guidelines referred to above.

The Data Protection Commissioners believe that data protection should be given the same priority as the promotion of data processing and telecommunications in the development and use of international data services. They therefore recommend that:

– Governments should move rapidly both individually and through international bodies towards establishing equivalent legal safeguards as soon as possible.

– Those transmitting personal data across national boundaries should check and monitor the protection given to such data by those receiving them, with a view to ensuring that proper regard will be given to the position of individuals.

The objective of these actions should be to ensure that:

– The Basic Principles for Data Protection contained in Treaty 108 and in the OECD guidelines are guaranteed to an individual notwithstanding the transfer of his data across national boundaries;

– Internationally operated data processing systems are structured in such a way that the individual can safeguard his data protection rights without undue difficulty;

– Any correction, up-dating and erasure applied to data which have previously been transmitted abroad will also be applied to the transferred data in any foreign country concerned;

– The greater risks, entailed by international exchanges of data, to the rights of individuals to decide on the use to be made of their data are counterbalanced by international co-operation among data protection commissioners.

Entschließung über die Arbeitsgruppe Telekommunikation und Medien

Die Ausarbeitung des Entwurfs für eine Entschließung war Anlaß zu einem sehr nützlichen Informationsaustausch zwischen den teilnehmenden Delegationen.

Die Empfehlungen und Entscheidungen, die wir in unseren jeweiligen Ländern ausgesprochen bzw. getroffen haben, sollten die internationale Dimension der Netze und Dienstleistungen berücksichtigen.

Die Informationen über die Entwicklungen, die sich jenseits unserer Grenzen vollziehen, dürfen uns nicht ausschließlich von unseren nationalen Organen übermittelt werden.

Die Netze und Dienstleistungen werden in unseren jeweiligen Ländern nicht gleichzeitig bzw. im selben Rhythmus weiterentwickelt.

Unsere Erfahrungen haben gezeigt, daß die Effizienz des Datenschutzes in diesem Bereich – über die Prinzipien hinaus – auf praktischen Maßnahmen beruht, über die von den nationalen Verwaltungsinstanzen Informationen nicht leicht zu erhalten sind.

Daher beschließt die Konferenz, daß diese Arbeitsgruppe ihre Arbeit in Berlin fortsetzt und daß nach Möglichkeit jede Delegation ihre Erfahrungen, insbesondere in folgenden Bereichen, einbringen sollte:

– detaillierte Rechnungslegung

– Modalitäten zur Aufnahme in die Teilnehmerverzeichnisse, Verwendung der Teilnehmerverzeichnisse

– verschiedene Kategorien der Telematischen Dienste (elektronische Post, Fernkäufe, Informationsdienste usw.)

– Fernmeßverfahren

– ISDN

– Zelluläres Telefon (digitaler Mobilfunk)

– automatische Anrufeinrichtungen

– Sicherheit der Netze

– Kabelnetze für Dialogfernsehen.

Resolution about the Working Group on Telecommunications and Media

When drafting the resolution on ISDN the delegations had a first, fruitful exchange of information.

When we express opinions or make decisions on our countries, we have to take into account the international dimension of telecommunication networks and services.

Information on events taking place beyond our national borders can not be provided to us by our national operators only.

Networks and services do not always develop at the same time and at the same place in our countries.

Experience has shown that the efficiency of data protection in this field depends – beyond mere principles – on practical measures and this is not always easy to obtain from our national operators.

This is why the Conference agrees that this Working Group should continue its work in Berlin.

Each delegation should have the opportunity to present its experiences in detail (analysis of the problems, possible solutions, adopted solutions) particular in the following fields:

– detailed bills

– provisions regarding the listing of subscribers in directories and the use of directories

– the different categories of telematic services (electronic mail, teleshopping, information services)

– telemetry

– ISDN

– cellular telephone (digital car telephone)

– automatic prerecorded message device

– network security

– interactive TV cable networks.

Beschluß zu ISDN auf Vorschlag der Arbeitsgruppe Telekommunikation und Medien

Die nationale und internationale Entwicklung der Telekommunikation ist derzeit gekennzeichnet durch die Einführung diensteintegrierender, digitalisierter Netze. Diese sind die Träger vielfältiger Dienste.

Die Entwicklung führt sowohl für die Netzträger als auch für die Diensteanbieter zur Verarbeitung von erheblich mehr personenbezogenen Daten, als dies bei bisherigen Netzen der Fall war. Diese Situation erfordert nationale und internationale Vorkehrungen zum Schutz personenbezogener Daten.

Die Internationale Konferenz der Datenschutzbeauftragten stellt fest, daß hierzu erhebliche Anstrengungen erforderlich sind. Insbesondere darf der Datenschutz nicht als Hindernis für die Entwicklung des Internationalen Informationsmarktes gesehen werden, sondern er stellt vielmehr eine notwendige Ergänzung der technischen Entwicklung dar, die für die Akzeptanz der neuen Telekommunikationstechnologien unerläßlich ist, er stellt vielleicht sogar ein beschleunigendes Element dieser Entwicklung dar.

Sie geht bei offenen Netzen von folgenden Grundsätzen aus:

– Abrechnungsdaten dürfen nur und nur so lange gespeichert werden, wie dies erforderlich ist, um Rechnungen zu erstellen oder auf eventuelle Anfechtungen zu reagieren; ferner zur Erstellung detaillierter Rechnungen, die ausschließlich für diejenigen Teilnehmer bestimmt sind, die sie angefordert haben. Die Vereinfachung der Tarifsysteme kommt dem Datenschutz entgegen.

– Für bestimmte Telekommunikationsdienste (Telefon, Kabelfernsehen mit Rückkanal, Datenübermittlungsdienste, Autobahngebühreneinzug usw.) müssen anonyme Zahleinrichtungen geschaffen werden. Ungeachtet der Abrechnungsprobleme macht es die Mehrwertigkeit der Netze erforderlich, diese mit den technischen Möglichkeiten eines anonymen Zugangs auszustatten.

– Daten, die für die Vermittlung erforderlich sind, sind unverzüglich zu löschen; Inhaltsdaten dürfen nur gespeichert werden, wenn sie für die Abwicklung des Dienstes erforderlich sind.

– Vorkehrungen sollten getroffen werden, die jenen Teilnehmern, die wünschen, in Teilnehmerverzeichnisse aufgenommen zu werden, garantieren, daß sie nicht Objekt unerwünschter kommerzieller Werbung werden. Das Recht, daß unentgeltlich in den Teilnehmerverzeichnissen kein Eintrag erscheint, sollte angestrebt werden. Daten, die die Erreichbarkeit von Teilnehmern sicherstellen

sollen, dürfen nicht zur Erstellung von Personenprofilen führen, die eine Verhaltenskontrolle erlauben.

– Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören oder zur Gewährleistung der Authentizität des Senders müssen auf höchstem technischen Niveau und zu akzeptablen Preisen angeboten werden.

– Angemessene Kontrollinstitutionen sind sowohl national als auch international einzurichten.

– In lokalen Netzen und bei Telekommunikationsendgeräten ist bereits bei der Normierung und Genehmigung auf den Datenschutz Rücksicht zu nehmen.

Insbesondere erfordern folgende Dienstemerkmale besondere Aufmerksamkeit:

– Die Anzeige des anrufenden Teilnehmers muß sowohl vom Anrufer als auch vom Angerufenen unterdrückt werden können; Mißbrauch muß durch Maßnahmen im Netz verhindert werden.

– Freisprecheinrichtungen müssen so gestaltet werden, daß nur mit Kenntnis der Gesprächsteilnehmer mitgehört oder aufgezeichnet werden kann.

– Beim Zugang zu Anrufbeantwortern, Voice- und Mailboxsystemen sowie Datenübermittlungsdiensten sind hinreichende Zugangssicherungen einzuführen.

Resolution on Integrated Services Digital Networks (ISDNs) Proposed by the Working Group on Telecommunications and Media

The present national and international development of telecommunications is characterized by the introduction of Integrated Services Digital Networks (ISDNs). These provide multiple services.

This development means that considerably more personal data is processed by network operators as well as by service suppliers than was the case with previous networks. This development calls far national and international measures to ensure the protection of personal data.

The International Conference of Data Protection Commissioners believes that considerable efforts are required in the light of this development. In particular, not only should data protection not be seen as an obstacle to the development of the international information market. On the contrary, it represents a necessary complement to the technical development, one which is essential to the accept-

ance of the new telecommunications technologies – it may even be an element that will accelerate this development.

In the case of open networks, data protection should be based on the following principles:

– Accounting data should be stored only if, and only for as long as it is essential for drawing up bills or responding to disputes about accuracy and furthermore itemised bills should be provided solely for those subscribers who request them.

– Anonymous payment procedures should be established for certain telecommunications services (telephone, cable TV with feedback channel, data transfer services, motorway toll etc.). Despite billing problems, the multipurpose character of the networks makes it necessary for them to be provided with the technical potential for anonymous access.

– Data necessary for establishing a circuit should be deleted immediatly. Other data may be stored only if it is essential for carrying out a service.

– Precautions have to be taken so as to ensure that those subscribers who want to be recorded in directories will not be subjected to undesired commercial advertising. The right to deletion without charge from subscriber directories should be an objective. Data collected and stored so that subscribers can be reached must not be used to draw up subscriber profiles allowing behaviour to be monitored.

– Data protection measures, in particular those to prevent unauthorised access, manipulation and interception, and those to authenticate the identity of the originator of a message must be provided to the highest possible technical standards and at an acceptable cost.

– Adequate regulatory institutions should be set up on both a national and international level.

– In the case of Local Area Networks and telecommunication terminals, data protection must initially be taken into account at the stages of setting design standards and approving equipment.

The following service features require particular attention:

– It must be possible for the identity of the caller to be suppressed by either the caller or the person being called. Abuse must be forestalled by provisions in the network.

– Installations for on-hook operating must be designed in such a way as guarantee that neither interception nor recording is possible without the concerned parties knowing about it.

– Access to answering machines, Voice- and Mailbox systems must be adequately secured.

1990

12. Konferenz, 19. September 1990, Paris

Probleme öffentlicher Telekommunikationsnetze und des Kabelfernsehens

Nachdem die Internationale Konferenz der Datenschutzbeauftragten in ihrer Entschließung vom 31. August 1989 allgemeine Grundsätze zu diensteintegrierenden digitalen Netzen (ISDN) aufgestellt hat, begrüßt sie den zweiten Bericht der Arbeitsgruppe „Telekommunikation und Medien“, der zeigt, daß diese Grundsätze konkretisiert und auf der technischen Ebene garantiert werden sollten. Diese Grundsätze sind auf jede Form der Telekommunikation einschließlich analoger Formen und bestimmter Formen massenmedialer Kommunikation (insbesondere Kabelfernsehen) anzuwenden. Öffentliche und private Netzbetreiber sollten diese Prinzipien ebenso verwirklichen wie Anbieter von Telekommunikationsdiensten.

I.
Teilnehmerverzeichnisse

Verzeichnisse von Teilnehmern an Telekommunikationsdiensten sind inzwischen weltweit die wichtigsten öffentlich verfügbaren personenbezogenen Dateien. Die Konferenz stellt mit Sorge fest, wie schwierig es ist, die Nutzung dieser Daten weltweit zu kontrollieren. Die Risiken nehmen durch den Verkauf der Teilnehmerverzeichnisse auf elektronischen Datenträgern zu.

Personenbezogene Daten, die von Netzbetreibern erhoben und gespeichert werden, müssen dem Zweck entsprechen, dem Betroffenen einen Telekommunikationsdienst zur Verfügung zu stellen und ihm den Zugang zum Netz zu ermöglichen; die Daten müssen für diesen Zweck erheblich sein und dürfen nicht darüber hinausgehen.

Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr

Geschlecht (und auf ihren Wohnort)* auszuschließen. Andererseits schließt dies die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus.

Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

Bei der Erhebung von Bestandsdaten sollte der Netzbetreiber den Betroffenen vollständig darüber aufklären, ob er zur Aufnahme seiner Daten in ein Teilnehmerverzeichnis unabhängig von der Form der Veröffentlichung verpflichtet ist oder nicht.

Bestandsdaten, die einen Mitbenutzer des Endgerätes betreffen, dürfen nur mit dessen Zustimmung in ein Teilnehmerverzeichnis aufgenommen werden.

Die Weitergabe von Bestandsdaten durch einen Netzbetreiber an Dritte zu Werbezwecken darf nur mit der freiwilligen und informierten Zustimmung des Betroffenen erfolgen, es sei denn, dieser hat nach innerstaatlichem Recht die Möglichkeit, der Weitergabe zu widersprechen.

Bestandsdaten von Teilnehmern, die einen Eintrag in das Teilnehmerverzeichnis ausgeschlossen oder sich entschieden haben, ihren Namen nicht für Werbezwecke nutzen zu lassen, sollten in keinem Fall an Dritte weitergegeben werden.

Besondere Aufmerksamkeit muß der höchsten räumlichen Ebene gewidmet werden, auf der dem Verzeichnis Teilnehmerdaten entnommen werden können.

Die Konferenz betrachtet mit Sorge die wachsenden Gefahren der telefonischen Direktwerbung und wird diese Probleme eingehender untersuchen.

II.
Anzeige der vom Anrufer benutzten Rufnummer

Die Einführung einer Einrichtung, die die Anzeige der Nummer des vom Anrufer benutzten Anschlusses am Endgerät des angerufenen Teilnehmers vor der Herstellung der Verbindung ermöglicht, wirft ernste Fragen des Schutzes der Privatsphäre auf.

Es ist wichtig, den Schutz der Privatsphäre des einzelnen Teilnehmers – der anrufenden und der angerufenen Person – mit den Erfordernissen der Kommunikationsfreiheit in Einklang zu bringen. Dies wird durch die Beachtung der folgenden Grundsätze erreicht:

* bezüglich des Klammerzusatzes bestehen unterschiedliche Auffassungen

Der Anrufer muß die Möglichkeit haben, durch eine einfache technische Vorrichtung im Einzelfall zu entscheiden, ob er seine Rufnummer anzeigen lassen will oder nicht, auf die Gefahr hin, daß sein Anruf von der angerufenen Person nicht entgegengenommen wird.

Dieses Verfahren zur Unterdrückung der Rufnummernanzeige muß für den Teilnehmer gebührenfrei sein.

Bei der Anwendung dieser Grundsätze sollen die folgenden Maßnahmen getroffen werden:

Teilnehmer müssen das Recht haben, gebührenfrei in das Teilnehmerverzeichnis einen Hinweis darauf aufnehmen zu lassen, daß sie kein Verfahren zur Anzeige der vom Anrufer benutzten Rufnummer anwenden.

Es ist notwendig, die Offenbarung übermittelter Informationen über den Anrufer an Dritte einzuschränken.

Ausnahmsweise darf die Unterdrückung der Rufnummernanzeige entsprechend dem innerstaatlichen Recht außer Kraft gesetzt werden, wenn Personen über Notruf die Feuerwehr oder den Notarzt anrufen.

Der Netzbetreiber kann die Unterdrückung der Rufnummernanzeige auch außer Kraft setzen, um auf Antrag der angerufenen Person den Urheber belästigender Anrufe festzustellen.

Diese Grundsätze sollen bei der Abwicklung internationaler Telefongespräche in gleicher Weise beachtet werden.

III.
Mobilfunk

Netzbetreiber, die ein Mobilfunknetz betreiben und anbieten, sollten Teilnehmer über die Sicherheitsrisiken informieren, die normalerweise – insbesondere bei fehlender Verschlüsselung der übermittelten Nachrichten – mit der Benutzung eines Mobilfunknetzes verbunden sind. Der Betreiber sollte dem Teilnehmer vor allem empfehlen, das Mobilfunknetz nicht zur Übermittlung vertraulicher Nachrichten zu benutzen, solange Probleme der Datensicherheit bestehen. Netzbetreiber sollten verpflichtet sein, den Teilnehmern am Mobilfunknetz wirksame Verschlüsselungsverfahren anzubieten.

Wirksame technische Vorkehrungen sollen getroffen werden, um den unbefugten Netzzugang über mobile Endgeräte zu verhindern.

Die Speicherung von Verbindungsdaten muß strikt auf den kurzen Zeitraum des Verbindungsaufbaus zwischen Teilnehmer und Netz beschränkt werden. Das Tarifsystem soll so gestaltet werden, daß die Orte, an denen Mobiltelefone benutzt worden sind, nicht Teil der Abrechnungsdaten sind. Besondere Beachtung verdient die Frage, inwieweit die Speicherung der vollständigen Rufnummer der angerufenen Person für Abrechnungszwecke notwendig ist.

IV.
Gebührenabrechnung

Inwieweit die Speicherung der vollständigen Nummer des angerufenen Teilnehmers für Zwecke der Gebührenabrechnung im allgemeinen erforderlich ist, sollte noch näher untersucht werden.

V.
Kabelfernsehen

Die Speicherung individueller Zuschauerprofile durch Kabelfernsehgesellschaften, die einzeln abrufbare („pay per view") Programme anbieten, ist ein Eingriff in die Privatsphäre des Kunden.

Deshalb sollten Kabelfernsehgesellschaften „pay per view"-Programme nur dann anbieten, wenn die Kunden eine praktikable und wirtschaftliche Möglichkeit (z. B. im voraus bezahlte Karten oder Decoder) haben, die Programme zu empfangen, ohne daß zuschauerbezogene Informationen gespeichert werden.

Messungen der Sehbeteiligung und Tantiemen dürfen nicht auf der Grundlage zuschauerbezogener Daten berechnet werden.

Die Konferenz befürchtet, daß in naher Zukunft im Bereich des Kabelfernsehens zahlreiche Datenschutzprobleme entstehen werden und wird die Entwicklung deshalb eingehend überwachen.

12th Conference, 19th September 1990, Paris

Resolution on Problems related to Public Telecommunication Networks and Cable Television

Having taken account of certain general principles on Integrated Services Digital Networks (ISDNs) in its resolution of 31st August 1989, the International Conference of Data Protection Commissioners welcomes the second report of the working group on "Telecommunications and Media" which indicates that these principles should be put in concrete terms and be guaranteed at the technical level.

These principles may be applicable to any kind of telecommunications including analogue forms as well as certain forms of mass media communication (especially cable television). Network operators in the public and the private sectors as well as firms offering telecommunications services should adhere to these principles.

I
Directories

Telecommunications directories happen to have become the most important publicly available personal data files in the world. The Conference notes with concern the difficulty in controlling the use of these data worldwide. The risks are enlarged by selling directory data on electronic media.

Personal data collected by a network operator should be adequate, relevant and nonexcessive with regard to the purpose of making available a telecommunications service to the data subject and connecting him to the network.

Personal data contained in a directory should be limited to such as are strictly necessary to identify reasonably a particular subscriber. He/she also has the right not to indicate his/her sex (and the place where he/she lives)*. On the other hand this would not exclude the publication of additional data at the request of the subscriber.

Subscribers have the right, free of charge and without having to give reasons, to have no personal data included in a directory.

When collecting basic data, a network operator should fully inform the data subject of whether or not he is obliged to have his data included in a subscriber directory regardless of the medium of publication.

Basic data relating to co-users of the subscriber's terminal may only be included in a directory with their consent.

The communication of basic data by a network operator to a third party for marketing purposes may only be carried out with the free and informed consent of the data subject unless the subscriber according to national law is given the opportunity to object.

Basic data of subscribers having refused to have their data included in a directory or having decided to have their name on a no-publicity list should not, in any case, be communicated to any third party.

* There are differing views as to the words in brackets

The Conference is concerned about the increasing dangers of direct marketing by telephone and will look into these problems in greater detail.

II
Calling line identification

The introduction of a service feature permitting the display of the number of the line used by the caller on the called subscriber's telephone before the connection is established raises serious questions of privacy.

It is important to reconcile the privacy requirements of the individual telecommunication user-caller and person being called with the requirements for freedom of communication. This is achieved through adherence to the following two principles:

– It must be possible for the caller to decide by simple technical means on a call-by-call basis whether he wants to be identified or not even at the risk of his call not being accepted by the called person.

– This non-identification procedure must be free of charge for the subscriber.

In application of these principles the following measures shall be taken:

Subscribers must have the right, free of charge, to indicate on the directory that they will not operate a procedure for identification of the calling line.

Regard should be had to the need to restrict disclosure of transmitted information concerning the caller to third parties.

As an exception, the suppression of the calling line identification may be overridden in case of persons calling emergency services such as fire brigades or ambulances according to national law.

The operator may also override the suppression of the calling line identification in order to trace malicious calls on request of the called person.

These principles shall be equally guaranteed when operating international calls.

III
Mobile telephones

When providing and operating a mobile telephone service, network operators should inform subscribers of the security risks which usually accompany the use of the mobile telephone network, particularly in the absence of encryption of

communications. The operator should advise the subscriber in particular that as long as problems of data security exist subscriber should refrain from using the mobile telephone network for the purpose of communicating confidential messages.

Network operators should be obliged to offer subscribers to the mobile telephone network effective encryption procedures.

Effective technical devices shall be introduced so as to prevent unauthorized access to the network.

The storage of traffic data must be strictly limited to the time required for connecting the subscriber to the mobile telephone network. The tariff system shall be designed in such a way that the locations where the mobile telephones have been used do not form part of the billing data.

IV
Billing

Further consideration should be given to the question as to what extent the storage of the complete number of the called person is necessary for billing purposes in general.

V
Cable television

The recording of individual viewing profiles by cable television companies offering "pay per view" programmes is an encroachment upon customers' privacy.

Therefore, cable television companies should only operate "pay per view" systems if a practical and economic opportunity is available to customers (e. g. prepaid cards or decoders) allowing them to receive the programmes without such information being recorded.

Audience ratings and royalties must not be calculated on the basis of identifiable viewers' data.

The Conference is concerned that in the field of cable television numerous data protection problems will arise in the near future and therefore will monitor developments in this area closely.

1991

13. Konferenz, 4. Oktober 1991, Straßburg

Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Telemarketing, der Kartentelefone und der elektronischen Directories und Beschluß der Internationalen Konferenz der Datenschutzbeauftragten

Bericht

Telemarketing

Der schnell zunehmende Gebrauch des Telefons für Zwecke der Direktwerbung (Telemarketing) bedroht die Privatsphäre der Verbraucher ernsthaft.

Es gibt zwei Hauptprobleme, die durch das Telemarketing für die Privatsphäre entstehen.

Das erste hängt mit der störenden Wirkung nicht erbetener telefonischer Verkaufsangebote auf die Verbraucher zusammen: Je öfter Anrufe für Werbezwecke entgegengenommen werden, desto störender wird der Verbraucher sie empfinden. Die Störung wird sogar noch verschärft, wenn die Anrufe von Anrufautomaten ausgelöst und durchgeführt werden.

Das zweite Problem betrifft die Nutzung von personenbezogenen Dateien, die für das Telemarketing eingesetzt oder als sein Ergebnis aufgebaut werden. Derartige Dateien können die informationelle Selbstbestimmung beeinträchtigen.

Telefonische Direktwerbung kann stattfinden:

a) im Zusammenhang mit einer bestehenden Beziehung zwischen dem Werbetreibenden und dem Verbraucher

und

b) wo keine derartige Beziehung besteht (cold calls).

Im Fall a), selbst solche Verbraucher, die im Rahmen einer bestehenden Beziehung angerufen werden, sollten das Recht haben, weiteren Anrufen zu widersprechen. Die Erfahrung in einigen europäischen Ländern hat gezeigt, daß Telefonpräferenzsysteme (Listen von Anschlußinhabern, die nicht für Werbezwecke angerufen werden wollen) nicht immer hinreichend wirksam die Privatsphäre schützen.

Im Fall b) sollten Verbraucher außerhalb einer bestehenden Geschäftsbeziehung nur angerufen werden, wenn diese Anrufe auf die Initiative des Verbrauchers zurückgehen.

Der Einsatz von Anrufautomaten sollte ohne die vorherige ausdrückliche Zustimmung des Verbrauchers nicht erlaubt sein, unabhängig davon, ob eine Geschäftsbeziehung besteht oder nicht.

Es sollten effektive Maßnahmen ergriffen werden, um unerwünschtes grenzüberschreitendes Telemarketing zu unterbinden.

Neue Techniken sollten nicht ohne Sicherungen zum Schutz der Privatsphäre eingeführt werden. Soweit diese Techniken Teilnehmerverzeichnisse benutzen, sollte den Teilnehmern an den neuen Diensten bereits bei Abschluß des Vertrages die kostenlose Möglichkeit eingeräumt werden, nicht in das Teilnehmerverzeichnis aufgenommen zu werden.

Diese Grundsätze sollten in gleicher Weise auf andere Telekommunikationstechniken wie Telefax oder Electronic Mail (elektronische Post) angewandt werden.

Die schnelle Entwicklung neuer Techniken zeigt, daß die Konferenz neue Entwicklungen sorgfältig beobachten sollte, um notwendige zusätzliche Maßnahmen zu empfehlen.

Kartentelefone

In den letzten Jahren sind elektronische Zahlungsmittel für das Telefonieren in öffentlichen Einrichtungen entwickelt worden.

Im Zusammenhang mit der Digitalisierung der Telefonnetze (bei der Einzelheiten des Anrufs im Netz gespeichert werden) ist die Möglichkeit des anonymen Zugangs zum Telefonnetz eine wichtige Sicherung der Privatsphäre.

Insofern ist die schnelle Entwicklung anonymer Telefonkarten auf Guthabenbasis, die in öffentlichen Telefonzellen benutzt werden können, sehr ermutigend.

Dennoch hat die internationale Mobilität des einzelnen – ergänzt durch Entwicklungen beim Mobiltelefon – dazu beigetragen, daß bestimmte Möglichkeiten angeboten werden, die die Anonymität herkömmlicher Telefonkarten entfallen lassen und dadurch Datenschutzprobleme erzeugen.

Diese Möglichkeiten führen dazu, daß identifizierbare Zahlungsmittel (Bankkarten, Kreditkarten, Telekarten) den Kunden vorzugsweise angeboten werden, ob-

wohl es keine unausweichlichen technischen oder organisatorischen Gründe gibt, um diese Alternative zu wählen.

Dementsprechend sollte auf internationaler Ebene besondere Aufmerksamkeit darauf verwendet werden, die Gestaltung, das Angebot und die Anbringung von Geräten zu fördern, die eine echte Auswahl zwischen den verschiedenen – anonymen oder identifizierbaren – Zahlungsmethoden ermöglichen.

Wenn der Einsatz eines identifizierbaren elektronischen Zahlungsmittels angeboten wird, muß besondere Aufmerksamkeit darauf verwendet werden, daß durch angemessene technische Maßnahmen Mißbrauch unterbunden wird. Insbesondere sollte es die Möglichkeit der Authentifizierung des Karteninhabers geben.

Schließlich sollten nur solche personenbezogenen Daten an die Kartengesellschaft übermittelt werden, die zur Rechnungsstellung erforderlich sind. Es sollte nicht möglich sein, von diesen Daten Rückschlüsse entweder auf die Nummer des Angerufenen oder den Ort des Telefons zu ziehen, von dem aus angerufen wurde.

Karteninhaber sollten vor Zweckentfremdung ihrer personenbezogenen Daten geschützt sein und auf angemessene Weise darüber informiert werden, welche Art von Daten das Kartentelefon erhebt und welche Art von Daten dem jeweiligen Diensteanbieter übermittelt wird.

Elektronische Post und damit zusammenhängende Teilnehmerverzeichnisse

Die Entstehung und schnelle Verbreitung der elektronischen Post unterstreicht, wie wichtig es ist, den Schutz personenbezogener Daten zu gewährleisten, die in elektronischen Teilnehmerverzeichnissen in Zusammenhang mit diesen Systemen gespeichert werden.

Die 12. Internationale Datenschutzkonferenz hat in ihrem Beschluß vom 19. September 1990 auf die Probleme hingewiesen, die bei öffentlichen Telekommunikationsnetzen und beim Kabelfernsehen insbesondere in bezug auf elektronische weltweite Teilnehmerverzeichnisse bestehen.

Nach eingehenderer Prüfung der Probleme elektronischer Teilnehmerverzeichnisse weist die Arbeitsgruppe auf folgende weitere Punkte hin:

Personenbezogene Daten sollten in derartigen Verzeichnissen nur mit der informierten Einwilligung des Teilnehmers gespeichert werden.

Betroffene sollten über spezielle Datenschutzrisiken informiert werden, die sich aus einem Eintrag in das Verzeichnis ergeben.

Die Identität der für das Verzeichnis verantwortlichen Stelle und der Umfang der personenbezogenen Daten, die für das Funktionieren des Verzeichnisses notwendig sind, sollten eindeutig festgelegt werden.

Technische Maßnahmen sollten getroffen werden können, um eine Verarbeitung (z. B. Umdrehen oder Kopieren des Verzeichnisses) zu unterbinden, die dem Datenschutz widerspricht.

Zusätzliche Probleme entstehen allerdings jetzt bei den Verzeichnissen, die im Zusammenhang mit Systemen der elektronischen Post geführt werden. Diese Probleme beziehen sich auf die Entstehung eines Verzeichnistyps, der völlig andere Eigenschaften besitzt als das herkömmliche elektronische Telefonbuch. Derartige Verzeichnisse sind gewöhnlich in Systemen der elektronischen Post eingebettet. Während sie viele Jahre lang vorhanden waren, haben die technischen Schwierigkeiten des Zugangs und der Manipulation solcher Verzeichnisse auf der normalen Nutzerebene ihre Wirkung aus datenschutzrechtlicher Sicht reduziert. Jetzt jedoch ist mit der Festlegung des X.500-Standards, dessen Hauptziel die Ermöglichung von Schnittstellen für Verzeichnisse aller Systeme der elektronischen Post ist, die Schaffung großer verteilter elektronischer Verzeichnisse technisch erleichtert worden, und die damit zusammenhängenden Datenschutzprobleme müssen gelöst werden.

Diese Probleme betreffen offensichtlich:

die Entstehung eines einheitlichen Personenkennzeichens für Eintragungen in das Verzeichnis (in der Literatur als „distinguished name“ bezeichnet). Die weltweite Erstreckung der geplanten Verzeichnisse unter dem X.500-Standard unterstreicht zusätzlich die Datenschutzprobleme, die mit einheitlichen Personenkennzeichen verbunden sind;

die verstärkten benutzerfreundlichen Möglichkeiten, die zur Verfügung gestellt werden für die Durchsuchung und Verarbeitung dieser Verzeichnisse;

Probleme im Zusammenhang mit der Möglichkeit, nicht in das Verzeichnis aufgenommen zu werden, da das Verzeichnis gerade die Aufgabe hat, den aktiven Betrieb der elektronischen Post zu gewährleisten.

Beschluß

Die 13. Internationale Konferenz der Datenschutzbeauftragten begrüßt den Bericht der Arbeitsgruppe Telekommunikation und Medien und unterstreicht die Bedeutung der beschriebenen Probleme in den Bereichen des Telemarketing, der Kartentelefone und der elektronischen Verzeichnisse.

13th Conference, 4th October 1991, Strasbourg

Report of the Working Group on Telecommunications and Media on problems relating to telemarketing, card telephones and electronic directories and Resolution of the International Conference of Data Protection Commissioners

Report

Telemarketing

The fast growing use of the telephone for direct marketing purposes (telemarketing) poses a serious threat to privacy of consumers.

There are two main privacy problems created by telemarketing.

The first relates to the intrusive effect of unsolicited sale calls on consumers: the higher the frequency of marketing calls received, the more a consumer might estimate these calls as being intrusive. The intrusiveness is even more increased when the calls are generated and executed by automatic calling devices.

The second problem concerns the use of personal data files which are used for, or created as a result of, telemarketing. Such files may involve an encroachment upon privacy.

Telemarketing calls can arise:

a) within the context of an existing relationship between the telemarketeer and the consumer

and

b) where no such relationship exists (cold calls).

In the case of a), even those consumers receiving calls within existing relationships should have the right to object to further calls. Experiences in some European countries have shown that telephone preference systems are not always sufficiently effective to protect privacy.

As regards b), calls to consumers where no previous relationship exists should only be made if the consumer has taken the initiative to receive such calls. The use of automatic calling devices should not be permitted without the previous expressed consent of the consumer irrespective of the existence of a relationship.

Consideration should be given to the etablishment of effective instruments in order to prevent undesirable transborder telemarking activities.

New techniques should not be introduced without safeguards with respect to the protection of privacy. To the extent that these techniques make use of directories, ex-directory facilities should be offered free of charge to the subscribers of the new services at the time of concluding the contract.

The principles outlined above should apply equally to other telecommunication techniques such as telefax or electronic mail.

The rapid development of new techniques indicates that the conference should keep a close eye on new developments with a view to proposing appropriate additional measures.

Card Telephones

Recent years have shown the appearance of electronic means of payment for telephone calls made from equipment available in public places.

In the context of the digitalization of telephone networks (with call details being stored within the network), the facility to access the telephone network anonymously represents an important privacy safeguard.

In this regard, the rapid development of the anonymous payment cards which can be used in public telephones is very encouraging.

Nevertheless, the mobility of individuals internationally coupled With developments in mobile telephony has contributed to the emergence of certain facilities which remove the anonymity associated with conventional telephone cards and thus give rise to data protection concerns.

These facilities involve identifiable means of payment (bank cards, credit cards, telecommunications cards) being offered to individuals on a preferential basis even though there are no inevitable technical or organisational reasons for choosing this particular option.

Accordingly, particular attention should be given at the international level, to encouraging the design, promotion and installation of equipment which permits a real choice between the different methods of payment, anonymous or identifiable.

When the use of an identifiable electronic means of payment is offered, particular attention needs to be given to ensuring that appropriate techniques are put into

place to prevent improper use. In particular, a means of authentication of the card user should be implemented.

Finally personal data transmitted to the card issuing company should be limited to that necessary for determining the bill. It should not be possible to deduce from such data either the called line number or the location of the telephone from which the call was made.

Card users should have safeguards against non-compatible uses of the data concerned and should be informed by appropriate means of the type of data collected by the equipment connected to the network, as well as the type of data transmitted to the service providers concerned.

Electronic Mail and Associated Directories

The emergence and rapid development of electronic mail facilities serves to underline the importance of tackling the data protection issues relating to personal data stored in the electronic directories which are associated with such systems.

The XIIth International Conference of Data Protection Commissioners, in its resolution of 19th September 1990 referred to problems related to public telecommunications networks and Cable television especially as far as electronic worldwide directories are concerned.

In developing its concerns about electronic directories, the Working Group would like to make the following further points:

Personal data should only be stored in such directories with the informed consent of the subscriber.

Data subjects should be informed about specific data protection risks arising out of an entry in the directory.

The identity of the controller of the directory and the scope of personal data necessary for the functioning of the directory should be clearly defined.

Technical measures should be available to forbid any processing (such as inversion or copying) which would contravene data protection policy.

Additional concerns now arise, however, in the area of directories associated with electronic mail systems. These relate to the emergence of a type of directory possessing characteristics quite unlike that of a conventional electronic telephone directory. Such directories are usually „embedded“ in electronic mail systems.

While in existence for many years, the technical difficulties in accessing and manipulating such directories at the ordinary user level has reduced their impact in data protection terms. Now, however, with the emergence of the X. 500 standard which focuses primarily on providing directory interfaces for all electronic mail systems, the establishment of large distributed electronic directories is technically facilitated and the associated data protection issues will require to be addressed.

These issues would appear to include:

The emergence of a unique personal identifier for entries in the directory (referred to in the literature as „the distinguished name"). The global nature of the proposed directories under the X. 500 standard further underlines the data protection concerns associated with unique personal identifiers.

The increased user-friendly facilities which will be made available for interrogation and processing of these directories.

Problems posed by the provision of „ex-directory" facilities because of the function of the directory in actively providing the mail service.

Resolution

The XIIIth International Conference of Data Protection Commissioners welcomes the report of the Working Group on Telecommunications and Media and notes the importance of the issues raised in the areas of telemarketing, phone card facilities and electronic directories.

1992

14. Konferenz, 29. Oktober 1992, Sydney

Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und Gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Bericht

Fernmeldegeheimnis

1.

Jeder Bürger, der ein Telefon benutzt, hat grundsätzlich die legitime Erwartung, daß sein Telefongespräch von niemandem, insbesondere von keiner staatlichen Stelle, abgehört wird.

Der Grundsatz der Vertraulichkeit von Telefongesprächen ist deshalb in den Verfassungen verschiedener Länder wie z. B. Österreichs, Deutschlands, Griechenlands, der Niederlande, Portugals und Spaniens verankert. Darüber hinaus garantiert die Europäische Menschenrechtskonvention das Recht jedes Einzelnen auf Achtung seiner Privatsphäre, seines Familienlebens, seiner Wohnung und seiner Korrespondenz. Dieser Artikel der Europäischen Menschenrechtskonvention ist vom Europäischen Menschenrechtsgerichtshof so ausgelegt worden, daß er auch das Fernmeldegeheimnis umfaßt.

In vielen Ländern ist das Abhören von Telefongesprächen sogar ein Straftatbestand. Die bloße Behauptung, daß Telefone illegal abgehört worden seien, kann auch weitreichende politische Konsequenzen haben. So mußte kürzlich ein Minister der Republik Irland auf Grund derartiger Vorwürfe zurücktreten, um nur ein Beispiel zu geben.

2.

Andererseits ist in den meisten Ländern anerkannt, daß es unter besonderen Voraussetzungen Ausnahmen vom Fernmeldegeheimnis geben muß. In Belgien, dem einzigen Land, in dem es bisher ein absolutes Verbot des Abhörens von Telefongesprächen gibt, bereitet die Regierung einen Gesetzentwurf für entsprechende Ausnahmen vor.

Die Statistik zeigt, daß Telefongespräche für Zwecke der Strafverfolgung im Jahre 1990 in 2449 Fällen in Deutschland und in 2031 Fällen in den Niederlanden abgehört wurden (Quelle: Bundesministerium für Post und Telekommunikation; Niederländisches Justizministerium).

Nach Art. 8 Abs. 2 der Europäischen Menschenrechtskonvention ist der „Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts" (auf Achtung des Post- und Fernmeldegeheimnisses) „nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist". Dieser Katalog von Ausnahmen, die der nationale Gesetzgeber vorsehen kann, ist sehr weitreichend, und einige europäische Länder haben restriktivere Vorschriften erlassen, die das Abhören von Telefongesprächen erlauben (vgl. auch Ziffer 2.4 des Entwurfs einer Empfehlung für den Schutz von personenbezogenen Daten im Bereich der Telekommunikationsdienste, mit besonderem Bezug zu Telefondiensten, angenommen vom Ausschuß für rechtliche Zusammenarbeit des Europarats, Juni 1992).

Die Arbeitsgruppe hat die neueren Entwicklungen der Gesetzgebung in den einzelnen Ländern untersucht und dabei festgestellt, daß trotz einiger Zweifel hinsichtlich der Effektivität des Telefonabhörens als Mittel im Kampf gegen die „organisierte Kriminalität" dennoch eine wachsende Tendenz zu beobachten ist, die Unverletzlichkeit des Fernmeldegeheimnisses mit zusätzlichen Ausnahmen zu versehen. In Deutschland trat in diesem Jahr ein neues Gesetz in Kraft, das eine Verwaltungsbehörde ermächtigt, Telefongespräche abzuhören, um illegale Waffenexporte zu verhindern (sogar bevor Straftaten begangen werden). In vielen Ländern kann das Telefonabhören in Strafverfahren angeordnet werden, die spezielle schwere Straftaten wie Drogenhandel, Mord und terroristische Verbrechen betreffen.

Allerdings wird das Abhören von Telefongesprächen neuerdings von Politikern auch als effektive Waffe im Kampf gegen Korruption und organisierte Kriminalität angesehen (Australien, Deutschland). Es ist bisher nicht gelungen, diese Kategorien von Straftatbeständen präzise zu beschreiben. Deshalb birgt jede Gesetzgebung, die mit derart ungenauen Tatbeständen arbeitet, die Gefahr, daß die Telefongespräche unverdächtiger Personen abgehört werden.

In Österreich wird andererseits über einen Gesetzentwurf diskutiert, der sogar den Geheimdienst verpflichtet, eine richterliche Anordnung zu beantragen, bevor Telefongespräche rechtmäßig abgehört werden dürfen.

Die Notwendigkeit einer Rechtsgrundlage für jeden staatlichen Eingriff in das Fernmeldegeheimnis hat der Europäische Menschenrechtsgerichtshof sehr strikt ausgelegt. In seiner neueren Rechtsprechung betont der Gerichtshof, daß Abhören und andere Formen der Registrierung von Telefongesprächen einen schwerwiegenden Eingriff in das Privatleben und die Kommunikation darstellen und deshalb auf einer Rechtsvorschrift beruhen müssen, die besonders präzise formuliert ist. Der Gerichtshof hebt hervor, daß es entscheidend ist, klare, detaillierte Vorschriften in diesem Bereich zu haben, insbesondere weil die verfügbare Technologie sich ständig weiterentwickelt (Fall Kruslin, 7/1989/ 167/223, Ziffer 33). Aus diesem Grund (Mangel an Präzision) wurde festgestellt, daß die Vorschriften des französischen Rechts über das Abhören von Telefongesprächen, gegen die Europäische Menschenrechtskonvention verstießen. Zwischenzeitlich ist Frankreich dem Beispiel des Vereinigten Königreichs gefolgt und hat ein neues Abhörgesetz verabschiedet, um den Anforderungen des Europäischen Menschenrechtsgerichtshofs zu entsprechen.

Das deutsche Bundesverfassungsgericht hat vor kurzem entschieden, daß eine präzise Rechtsgrundlage notwendig ist, um Fangschaltungen vorzunehmen, auch wenn der Inhalt der belästigenden Anrufe nicht aufgezeichnet wird.

Man kann drei Verfahrensstadien unterscheiden, wenn staatliche Stellen Telefone überwachen wollen:

– die Entscheidung, Telefongespräche abzuhören;

– die Durchführung dieser Entscheidung und

– die Kontrolle dieser Überwachungsmaßnahme, nachdem sie beendet worden ist.

Die Entscheidung, Telefongespräche abzuhören, kann getroffen werden von einer Verwaltungsbehörde (im Vereinigten Königreich), von einem Untersuchungsrichter (in den meisten Ländern) oder von einer Verwaltungsbehörde bzw. einem Gericht, je nachdem zu welchem Zweck abgehört werden soll (Deutschland). Beauftragte für den Datenschutz und den Schutz der Privatsphäre sind an diesen Entscheidungen nicht beteiligt und haben keine Kompetenz, sie zu überwachen. Dies bezieht sich ebenso auf die Durchführung der Anordnung, Telefongespräche abzuhören.

Sobald allerdings die Abhörmaßnahme beendet worden ist, gibt es gute Gründe dafür, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die Befugnis erhalten, die Nutzung der Daten zu kontrollieren, die aus der Abhörmaßnahme stammen. In einigen Ländern wächst die Erkenntnis, daß Beauftragte für den Datenschutz und den Schutz der Privatsphäre eine wichtige Rolle in die-

sem Bereich zu spielen haben, obwohl sie bisher noch keine derartige Kompetenz haben mögen.

In den Niederlanden wird das Recht möglicherweise in naher Zukunft in der Weise geändert, daß die Ergebnisse einer Abhörmaßnahme in den Akten der Nachrichtendienste dokumentiert werden. Sobald dies geschieht, würden diese Akten der Kontrollkompetenz der Registratiekammer unterliegen.

In Deutschland kann der Bundesbeauftragte für den Datenschutz nicht in ein gerichtliches Verfahren eingreifen, das zu einer Abhöranordnung führt. Aber der Bundesminister für Post und Telekommunikation hat anerkannt, daß der Bundesbeauftragte für den Datenschutz zu kontrollieren hat, ob die Deutsche Bundespost TELEKOM die Abhöranordnung korrekt durchführt, welche Art personenbezogene Daten bei Durchführung der richterlichen Anordnung erhoben werden und für welchen Zweck sie genutzt werden. Es ist entscheidend, daß die Ergebnisse einer Abhörmaßnahme nur für den Zweck benutzt werden, für den die Daten ursprünglich erhoben wurden.

In mehreren Ländern wird das Recht geändert, um die Überwachung von Nachrichten zu ermöglichen, die mit anderen Telekommunikationsmitteln (Telefax, Telex, Datenübertragung etc.) übermittelt werden. Zum Teil wird diese Gesetzgebung sich auch auf private Netzbetreiber und Diensteanbieter erstrecken und sie zur Zusammenarbeit mit der Polizei verpflichten.

Man muß sich vergegenwärtigen, daß die Überwachung von Telekommunikationsverbindungen, insbesondere das Abhören von Telefongesprächen, kein gewöhnliches Überwachungsmittel ist, das automatisch gegen jeden eingesetzt werden kann, der bestimmte Verbrechen begeht oder die nationale Sicherheit bedroht. Es ist im Gegenteil in den meisten Ländern eine Ermittlungsmethode für Ausnahmesituationen und unterliegt zusätzlichen Bedingungen. In einer Reihe von Ländern kann die Überwachung von Telefongesprächen nur angeordnet werden, wenn jemand einer Straftat verdächtigt wird, zu deren Aufklärung die Abhörmaßnahme beitragen kann, und nur dann, wenn herkömmliche Ermittlungsmethoden unpraktikabel oder erfolglos sind.

Es ist entscheidend, daß die Person, deren Telefongespräche abgehört worden sind, von der verantwortlichen Behörde über die Abhörmaßnahme informiert wird, sobald dies möglich ist, ohne den Zweck der Ermittlungen zu gefährden.

Nur dann ist der Einzelne in der Lage, die Abhörmaßnahme durch einen Richter oder ein anderes unabhängiges Organ überprüfen zu lassen. Die Benachrichtigung des Betroffenen ist bisher allerdings nur in wenigen nationalen Rechtssystemen vorgesehen.

3.

Das Recht des Bürgers, das Telefon zu benutzen, ohne registriert und beobachtet zu werden, schützt ihn nicht nur gegen die Aufzeichnung der Gesprächsinhalte, sondern auch gegen die Nutzung der technischen Daten, die vom Telekommunikationsnetz für andere als Abrechnungszwecke erzeugt werden (Verbindungsdaten wie Zeit, Dauer des Gesprächs und Rufnummer des Angerufenen). Allerdings gibt es von diesem Grundsatz noch weiterreichende Ausnahmen als vom Prinzip der Vertraulichkeit des Gesprächsinhalts. In Belgien und Deutschland können Verbindungsdaten auf Grund einer strafgerichtlichen Anordnung in jedem Strafverfahren genutzt werden, während das Abhören von Telefongesprächen im eigentlichen Sinn in vielen Ländern nur bei bestimmten Katalogstraftaten zulässig ist.

Auch in dieser Beziehung lassen sich in den verschiedenen Rechtssystemen unterschiedliche Tendenzen feststellen. In Australien hat der Attorney-General vor kurzem vorgeschlagen, den Begriff der Kommunikationsüberwachung neu zu definieren, so daß er das Mithören oder Aufzeichnen von Informationen umfaßt, die eine Person einer anderen über ein Telekommunikationssystem übermittelt, ohne das beide Gesprächsteilnehmer davon wissen; die Registrierung von Verbindungsdaten sollte nicht mehr unter diesen Begriff fallen. Diesen Vorschlag hat der australische Beauftragte für den Schutz der Privatsphäre scharf kritisiert. Nach seiner Auffassung sollten Verbindungsdaten und Inhaltsdaten, die über ein Telefonnetz übermittelt werden, in der gleichen Weise geschützt werden. Aufgrund neuerer technischer Entwicklungen (insbesondere der Einrichtung von digitalen Telekommunikationsnetzen) werden Verbindungsdaten systematisch von den Netzbetreibern gespeichert und sind deshalb für eine gewisse Zeit auch für andere Zwecke wie Strafverfahren verfügbar. Es gibt keinen Grund für ein unterschiedliches Schutzniveau für Inhaltsdaten einerseits und Verbindungsdaten andererseits. Der Grundsatz der Vertraulichkeit von Telefongesprächen schützt sowohl deren Inhalt als auch deren nähere Umstände (Zeit, Dauer und die an ihnen beteiligten Personen).

Aus demselben Grund hat die deutsche Konferenz der Datenschutzbeauftragten den Bundestag aufgefordert, die alte Vorschrift aufzuheben, die die Nutzung von Verbindungsdaten für jedes Strafverfahren zuläßt. Wendet man diese Vorschrift auf digitale Netze an, so ist sie mit dem verfassungsrechtlich geschützten Fernmeldegeheimnis nicht mehr vereinbar.

4.

Da die Gesetzgebung über die Telekommunikationsüberwachung gegenwärtig in vielen Ländern, die in der Arbeitsgruppe vertreten sind, geändert wird, kann dieser Bericht nur ein Zwischenbericht sein. Es ist notwendig, daß die Beauftragten für den Datenschutz und den Schutz der Privatsphäre die technische und rechtli-

che Entwicklung in diesem Bereich genau beobachten, um die Privatsphäre des Einzelnen gegen exzessive Überwachung zu schützen.

Satellitenkommunikation

Vor mehr als sechs Jahren verabschiedete die VII. Internationale Konferenz der Datenschutzbeauftragten in Luxemburg eine Entschließung über Datenschutz und Neue Medien, in der sie betonte, daß der „Einsatz von Satelliten zur Kommunikation"… „Im Hinblick auf die Datenintegrität und den Schutz vor unbefugtem Abhören ebenfalls Risiken" schafft.

Seitdem scheinen diese Risiken fast vergessen, obwohl es geradezu eine Revolution am Himmel gegeben hat, was die Kapazität der Satelliten angeht. Der Kapazitätszuwachs der europäischen Satelliten von 1989 bis 1993 wird bei 215 % liegen (vgl. EG-Kommission, Grünbuch zur Satellitenkommunikation, Tabelle 5, S. 57).

Satelliten können für eine Reihe von Zwecken eingesetzt werden, deren wichtigste die Verteilung von Fernsehprogrammen und die Telekommunikation sind. Es gibt andere Einsatzmöglichkeiten wie etwa die weltweite

– Positionsbestimmung und das Flottenmanagement,

– Fernmessen und Fernwirken,

– Fernerkundung.

1. Telekommunikation

Ein Satellitensystem besteht in der Regel aus mindestens zwei Erdfunkstationen und dem Raumsegment. Informationen werden von einer leistungsstarken Erdfunkstation zum Satelliten gefunkt („Uplink", Aufwärtsstrecke; ein fester Punkt-zu-Punkt-Dienst). Sie werden dann über Transponder im Satelliten zurück zu einer anderen Erdfunkstation oder mehreren Erdfunkstationen übermittelt („Downlink", Abwärtsstrecke). Bei der Abwärtsstrecke sind verschiedene Dienstformen vorstellbar, wie z. B. ein fester (Punkt-zu-Punkt-Telekommunikations-) Dienst, ein Fernsehverteil-(Punkt-zu-Mehrfachpunkt-) Dienst, ein mobiler Dienst, bei dem Informationen zu beweglichen Empfangsstationen wie etwa Lastwagen mit kleinen Dachantennen gefunkt werden. Moderne Satelliten tragen bis zu 16 Transponder und jeder Transponder kann bis zu zwei Fernsehkanäle oder 1 700 Telefonsprachkanäle übertragen.

In Europa werden nur 2 bis 3 % der internationalen Telefongespräche über Satellit abgewickelt, während Satelliten eine weit größere Rolle bei transatlantischer und

interkontinentaler Telekommunikation spielen, wo sie fast 60 % des Verkehrsaufkommens übernehmen. Satellitengestützte Kommunikationsnetze sind von großer Bedeutung für den Aufbau der Telefoninfrastruktur in Ost- und Zentraleuropa. Die Entwicklung von billigen Antennen mit einem Durchmesser von weniger als einem Meter, insbesondere VSATs (Very Small Apperture Terminals, auch Mikrostationen genannt), die schon in den Vereinigten Staaten weit verbreitet sind, erleichtert neue Punkt-zu-Mehrfachpunkt-Dienste. Die Unterscheidung zwischen Individual- und Massenkommunikation verschwimmt immer mehr. Mikrostationen können reine Empfangs- oder interaktive Empfangs- und Sendeterminals sein. Diese technische Entwicklung führt zur Entstehung von weltweiten mobilen „Overlay"-Telekommunikationsnetzen. Sie werden terrestrische Mobilfunknetze, die in dicht besiedelten Gebieten bestehen, ergänzen, allerdings nicht ersetzen. Satellitenkommunikation wird besondere Bedeutung in großen, dünn besiedelten Ländern wie Australien, Kanada und Rußland haben.

Das Raumsegment eines Satellitensystems steht im Eigentum einer internationalen Organisation wie z. B INTELSAT (International Telekommunications Satellite Organisation), EUTELSAT, INMARSAT (International Maritime Satellite Organisation), American Mobile Satellite Corporation (USA), TELESAT MOBILE (Kanada) oder AUSSAT (Australien). Dabei handelt es sich um kommerzielle Organisationen auf der Grundlage von zwischenstaatlichen Verträgen, die selbst allerdings keine Völkerrechtssubjekte sind. Alle Unterzeichnerstaaten haben einen gewissen Kapitalanteil an der Organisation. Die Satellitenorganisationen verkaufen Kapazitäten im Raumsegment entweder selbst oder durch Diensteanbieter.

Neue Dienste vor allem für geschlossene Benutzergruppen umfassen:

a) INTELSAT Business Service (IBS), der Sprachübermittlung, Fax, Telex, Datenübertragung, elektronische Post und Videokonferenzen integriert,

b) INTELNET-Dienste, die auf Datenverteilung und Datensammlung beschränkt sind,

c) nationales oder weltweites satellitengestütztes Paging.

Geostationäre Telekommunikationssatelliten (also Satelliten, die sich in einer gleichzeitigen Umlaufbahn zur Erdoberfläche bewegen), die gegenwärtig in Betrieb sind, reflektieren lediglich die Daten, die zu ihnen heraufgefunkt werden, auf einer anderen Frequenz hinunter zu einer anderen Erdfunkstation.

Eine neue Satellitengeneration könnte allerdings durchaus auf andere Weise arbeiten: Nicht-geostationäre Satelliten können Informationen von einem Punkt der Erdumlaufbahn zu einem anderen transportieren, was die Speicherung von Daten

im Raumsegment über eine längere Zeit erforderlich machen würde, als für das bloße Reflektieren der Daten erforderlich ist. Ein deutscher Forschungssatellit, der gegenwärtig Wissenschaftlern in der Arktis dient, funktioniert auf diese Weise (wie ein Postbote).

Sobald Daten im Raumsegment verarbeitet werden, wachsen die klassischen Risiken für die informationelle Selbstbestimmung, die mit jeder Verarbeitung von personenbezogenen Daten verbunden sind. Die EG-Kommission hat erkannt, daß satellitengestützte Kommunikation sowohl nationale wie auch EG-Gesetzgebung umgehen kann. Allerdings hat die Kommission bisher kein überzeugendes Konzept entwickelt, wie diesen Risiken zu begegnen ist.

2. Positionsbestimmung und Flottenmanagement

Satelliten werden zunehmend für Zwecke der Navigation nicht nur von Schiffen (die das INMARSAT-System nutzen), sondern auch von Lastwagen und sogar Einzelpersonen genutzt.

EUTELTRACS ist ein europäisches satellitengestütztes System für die mobile Landkommunikation zum Management von LKW-Flotten. Die Position eines Fahrers und seine Bewegungen mit dem LKW können von einer Zentralstelle zu jeder Zeit überprüft werden. Dies spart für das Unternehmen Zeit und Geld und könnte auch zur Vermeidung von Verkehrsstauungen beitragen, wenn die Zentralstelle den Fahrern alternative Routen vorschlagen kann, die weniger überfüllt sind.

Das Global-Positioning-System (GPS – globales Positionsbestimmungssystem) wurde vom Pentagon entwickelt und erfolgreich im Golfkrieg getestet. Es beruht auf gegenwärtig 16 Satelliten (Ende 1993 werden es 21 sein), von denen jeder die genaue Zeit und Position aussendet, die von jedem, der mit einem GPS-Empfänger ausgerüstet ist, empfangen werden kann. Der Empfänger wiederum berechnet seine genaue Position im Verhältnis zum Satelliten. Dieses System erlaubt z. B. einer Reederei, den Standort jedes ihrer Schiffe weltweit zu ermitteln und dann Informationen an das Schiff über INMARSAT zu übermitteln. Piloten und in naher Zukunft auch Fahrer können das System zusammen mit digitalen Landkarten benutzen, um ihren Weg in unbekannter Umgebung zu finden.

Gleichzeitig ist es offensichtlich, daß mit einem solchen System ein elektronisches Bewegungsprofil des Einzelnen ohne dessen Einwilligung erzeugt werden kann.

3. Fernmessen und Fernwirken

Satellitengestützte Netze können auch genutzt werden, um Pipelines, Eisenbahnlinien, Stromleitungen und Ölquellen zu überwachen. Mit Hilfe der Fernmeß-

technik kann sogar die Temperatur in einem Kühlwagen kontrolliert und angepaßt werden. Zugleich würde dies auch eine verstärkte Überwachung der Arbeitnehmer bedeuten.

4. Fernerkundung

Fernerkundung ist eine ältere (ursprünglich militärische) Einsatzform von Satelliten, durch die Bodenschätze, Wolkenbildungen (für die Wettervorhersage) Umweltverschmutzung und sogar die Routen von Zugvögeln vom Himmel aus beobachtet werden können.

Im Jahre 1991 startete die European Space Agency (ESA) einen modernen Satelliten (ERS-I), um Umweltveränderungen zu erkunden. Dieser Satellit verfügt über ein Radarsystem (SAR-Synthetic Aperture-Radar), das in der Lage ist, sogar nachts oder durch eine geschlossene Wolkendecke Fotografien der Erdoberfläche zu machen. Dieser Satellit speichert bestimmte Daten, bis er eine Position erreicht, von der aus er sie zu der nächsten Erdfunkstation abstrahlen kann.

Fernerkundungssatelliten, die von den alliierten Streitkräften im Golfkrieg eingesetzt wurden, waren in der Lage, Objekte (z. B. Panzer) zu erkennen, die zwischen 1 und 5 Metern Kantenlänge hatten. Es ist sehr wahrscheinlich, daß Satellitentechnologie, die von den Militärs entwickelt wurde, mit einer gewissen zeitlichen Verzögerung auch für den zivilen Einsatz verfügbar sein wird.

Die EG-Kommission plant, über Satellit zu kontrollieren, ob Landwirte eine geringere Menge einer bestimmten Getreideart anbauen, als die, für die sie Gemeinschaftszuschüsse erhalten. Die Technik wird bald verfügbar sein, z. B. mit Hilfe eines Satelliten die Schlagzeilen einer Zeitung zu lesen, die jemand an einer Bushaltestelle liest.

5.

Die unbestrittenen Vorteile der Satellitentechnologie werden begleitet von offensichtlichen Risiken für die Privatsphäre, sobald der Einzelne ins Blickfeld des Satelliten gerät. Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre sollten sich deshalb für internationale Abkommen einsetzen, die regeln,

– in welchem Ausmaß personenbezogene Daten im Weltall verarbeitet werden dürfen,

– wer der verantwortliche Datenverarbeiter ist, wenn personenbezogene Daten im Raumsegment gespeichert werden, und wer für die Datensicherheit verantwortlich ist,

– daß besondere technische Maßnahmen ergriffen werden müssen, z. B. sollten Verschlüsselungstechniken (die bereits im militärischen Bereich angewandt werden) für die zivile Nutzung ohne zusätzliche Kosten angeboten werden.

Der internationale Normungsprozeß für weltweite Mobilkommunikation über Satellit berücksichtigt den Datenschutz noch immer nicht hinreichend.

Gemeinsame Erklärung

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre, die sich zu ihrer XIV. Internationalen Konferenz in Sydney getroffen haben,

– begrüßen den Bericht der Arbeitsgruppe Telekommunikation und Medien,

– heben die Bedeutung der beschriebenen Probleme im Bereich des Fernmeldegeheimnisses und der Satellitenkommunikation hervor und

– stimmen darin überein, daß die technische und rechtliche Entwicklung im Bereich des Fernmeldegeheimnisses sorgfältig beobachtet werden muß, um die Privatsphäre des Einzelnen vor exzessiver Überwachung zu schützen.

14th Conference, 29th October 1992, Sydney

Report of the Working Group on Telecommunication and Media on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the International Conference of Data Protection and Privacy Commissioners

Report

Secrecy of Telecommunications

1.

Every citizen making a telephone call has in principle the legitimate expectation that his telephone conversation will not be intercepted by anybody, especially by public authorities.

The principle of the inviolability of telephone conversations is therefore guaranteed in the constitutions of several countries such as Austria, Germany, Greece, The Netherlands, Portugal and Spain. Moreover, the European Convention on Human Rights guarantees everyone's right to respect for his private and family life,

his home and his correspondence. This provision of the European Convention has been interpreted by the European Court of Human Rights as covering the secrecy of telephone conversations.

In many countries the interception of telephone communications is even regarded as a criminal offence. The mere allegation of illegal telephone tapping can also have far-reaching political consequences. Recently a Minister in the Irish Republic had to step down due to such allegations, to give but one example.

2.

On the other hand, it has always been accepted in most countries that under special conditions there have to be exemptions from the principle of the secrecy of telephone conversations. In Belgium as the only country with an absolute legal prohibition to intercept telephone conversations the government is preparing a bill allowing for equivalent exemptions.

Statistics show that telephone conversations have been tapped for purposes of criminal procedure in 1990 in 2 449 cases in Germany and in 2 031 cases in the Netherlands (Source: German Federal Minister for Post and Telecommunications; Dutch Ministry of Justice).

According to Article 8, 2 of the European Convention on Human Rights "there shall be no interference by a public authority with the exercise of . . . 'the right to respect for the secrecy of correspondence and telephone conversations' … except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". This catalogue of legal exemptions which the national legislature may provide for is very far-reaching and some European countries have adopted more restrictive rules to allow for telephone tapping (cf. also para. 2.4 of the Draft Recommendation on the Protection of Personal Data in the Area of Telecommunications Services, with Particular Reference to Telephone Services, adopted by the Council of Europe's Committee on Legal Co-operation (CDCJ), June 1992).

When studying recent developments in the national legislation the Working Group has noticed that although there may be some doubts as to the effectiveness of telephone tapping in so far as it is related to "organized crime" there is nevertheless a growing tendency to allow for additional exemptions to the principle of the inviolability of telephone communications. In Germany new legislation came into force this year authorizing an administrative body to tap telephone conversations in order to prevent illegal arms exports (even before criminal offences have been committed). In many countries telephone tapping can be initiated in criminal

proceedings concerning specific serious crimes such as drug trafficking, murder and terrorist offences.

However, recently telephone tapping is seen by politicians as an effective weapon against "official corruptions" and "organized crime" (Australia, Germany). These categories of offences have not yet been and cannot be precisely defined. Therefore any legislation incorporating these imprecise categories involves the risk that unsuspected persons have their telephone calls intercepted.

Austria on the other hand introduced legislation obliging even the Secret Service to obtain a judicial order before telephone conversations can be tapped legally.

The need for a legal basis for any interference by a public authority with the right to secrecy of telecommunications is being interpreted very restrictively by the European Court of Human Rights. In its most recent jurisprudence the Court stressed that tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. The Court stressed that it was essential to have clear, detailed rules on the subject, especially as the technology available for use was continually becoming more sophisticated (Kruslin case, 7/1989/ 167/223, para. 33). For this reason (lack of precision) the French law governing telephone tapping was found contravening the European Convention on Human Rights. In the meantime France has followed the example of the United Kingdom and has passed a new act governing telephone tapping in order to meet the European Court's requirements.

The German Federal Constitutional Court has recently ruled that a precise legal basis is necessary to trace malicious calls, even if their contents are not being recorded.

There are three stages to be distinguished when telephones are to be monitored:

– the decision to intercept telephone communications;

– the implementation of that decision and

– the supervision of this surveillance measure after it has ended.

The decision to intercept telephone conversations may be taken by an administrative body (in the United Kingdom), by an organ of judicial investigations (in most countries) or by an administrative or a judicial authority depending on the purpose of the tapping (Germany). Data Protection and Privacy Commissioners are not involved in these decisions and have no jurisdiction to control them. This applies equally to the implementation of the surveillance order.

However, once the interception of telephone communications has stopped, there is a strong case for Data Protection and Privacy Commissioners to be able to control the use of data stemming from the tapping of telephone calls. In some countries there is a growing consciousness that Data Protection and Privacy Commissioners have an important role to play in this field although they may not yet have jurisdiction to that effect.

In the Netherlands the law may be changed in the near future so that results from telephone tapping will be recorded by the Criminal Intelligence Services in their files. Whenever in the Netherlands results from telephone tapping should be recorded in files – for instance in files held by the Criminal Intelligence Services – they would come under the competence of the Registration Chamber.

In Germany the Federal Data Protection Commissioner cannot interfere with the judicial proceedings leading to an order to intercept telecommunications. But the Federal Ministry for Post and Telecommunications has accepted that the Data Protection Commissioner controls whether the German TELEKOM carries out the court order properly, what kind of personal data are being collected when carrying out the court order and for which purpose they are used. It is essential that results of a surveillance measure are only used for the purpose for which the data were originally collected.

In several countries the law is or will be amended to allow for the interception of messages transmitted by other means of telecommunications (telefax, telex, data transmission etc.). Some of the legislation will also cover private network operators and service providers obliging them to cooperate with the police as required.

One must keep in mind that the interception of telecommunications, especially telephone tapping is not a usual means of Surveillance, automatically available against anyone committing certain crimes or causing a threat to national security. On the contrary, in most countries it is an exceptional method of investigation and is subject to additional conditions. In a number of countries the surveillance of telephone calls may only be ordered if someone is suspected of an offence which tapping can help to investigate and only if traditional methods of inquiry are impractical or have failed.

It is essential that the person whose telephone calls have been intercepted is notified by the public authority responsible of the fact that he has been subject to surveillance as soon as practicable without prejudicing the purpose of the surveillance.

Only then is the individual in a position to apply for a review of the measure by a judicial or another independent body. This notification of the data subject is so far only provided for in a few national legal systems.

3.

The right of the citizen to use the telephone without being registered and observed does not only protect him against the interception of the contents of his conversation but also against the use of the technical data generated by the telecommunications network (traffic data such as time, duration of the call and number of the called party) for other than billing purposes. However, the exemptions to this rule are even more wide-ranging than to the rule of confidentiality of the contents of the telephone conversation. In Belgium and in Germany such technical (metering) data may be used by in order of the investigating judge in criminal proceedings of any kind whereas telephone tapping in the narrower sense is in many countries restricted to a catalogue of specific crimes.

Again in this respect diverse tendencies can be noted in different legal systems. In Australia the Attorney – General's Department recently proposed to redefine the interception of a Communication to cover the listening to or recording of messages passing from one person to another over a telecommunications system without the knowledge of either party thereby excluding personal informations generated by the system itself (traffic data). This proposal has been strongly criticized by the Australian Privacy Commissioner. In his view traffic data and Signals information should be protected in the same way as the Contents of messages conveyed across the telephone network. Due to recent technological developments (especially the installation of digital telecommunications networks) traffic data are being systematically stored by the network operators and therefore during a certain period of time available for other purposes such as criminal proceedings. There is no reason for a different level of protection of the content data as opposed to the traffic data. The principle of secrecy of telephone conversations covers both their contents and their circumstances (time, duration and persons taking part in it).

For the same reason the German Conference of Data Protection Commissioners has urged the German Federal Parlament to repeal the old provision which allows for the use of traffic data for any criminal proceedings. When applied to digital networks that provision is no longer in line with the constitutional guarantee of secrecy of telecommunications.

4.

As the legislation regarding the interception of telecommunications is currently being amended in many countries that are represented in the Working Group this report can only be an interim report. It is necessary for the Data Protection and Privacy Commissioners to keep a close eye on the technological and legal developments in this field in order to protect the privacy of the individual against excessive state surveillance.

Satellite Communications

More than six years ago the VIIth International Conference of Data Protection Commissioners in Luxembourg passed a resolution on Data Protection and New Media stressing that the "use of satellites for communication likewise induces risks with regard to data integrity and protection against unauthorised monitoring".

Since then these risks seem to have been almost forgotten although there has been a virtual revolution in the skies as far as the capacity of satellites is concerned. The increase in capacity of European satellites from 1989 to 1993 will be 215 % (cf. EC Commission, Green Paper on satellite communications, Figure 5, p. 57).

Satellites can be used for a number of purposes, the most important being broadcasting and telecommunications. There are other possible applications such as worldwide

– positioning and fleet management,

– telemetry and remote controlling,

– remote sensing.

1. Telecommunications

A satellite system usually consists of at least two earth stations and the space segment. Information is beamed up from a high-powered earth station to the satellite ("uplink", a fixed point-to-point service). It is then re-transmitted by transponders on the satellite back to another earth station or several earth stations ("downlink"). The downlink can be specified in terms of services, such as a fixed (point-to-point telecommunications) service, a broadcasting (point-to-multipoint TV distribution) service, a mobile service, which beams down to moving receiving stations, such as trucks with roof-top antenna dishes. Modern satellites carry up to 16 transponders and each transponder can transmit up to two TV-channels or 1 700 telephone voice channels.

Within Europe only 2 % – 3 % of international telephone calls are made via satellite whereas satellites play a far greater role in transatlantic and intercontinental telecommunications accounting for nearly 60 % of traffic. Satellite communications networks are of great importance for the build-up of the telephone infrastructure in Eastern and Central Europe.

The emergence of low-cost terminal dishes (antennas) with diameters of less than 1 metre, especially VSATs (Very Small Aperture Terminals, also called microsta-

tions), which are already Widespread in the United States, facilitates new point-to-multipoint services. The distinction between individual telecommunications and broadcasting becomes increasingly blurred, Microstations may be receivers only or receive/ transmit terminals (interactive). This technological development will lead to the emergence of world-wide mobile telecommunications "overlay" networks supplementing (not replacing) terrestrial cellular networks which are concentrated on densely populated areas. Satellite telecommunications will be especially important in large thinly populated countries such as Australia, Canada and Russia.

The space segment of a satellite system is owned by an international organisation such as INTELSAT (International Telecommunication Satellite Organization), EUTELSAT, INMARSAT (International Maritime Satellite Organization), American Mobile Satellite Corporation (USA), TELESAT Mobile (Canada) or AUSSAT (Australia). They are commercial organisations based on international treaties but they are not international legal persons themselves. All signatory states have a certain capital share in the organisation. The satellite organisations sell space segment capacity either themselves or through service providers.

New services especially for closed user groups include:

a) INTELSAT business service (IBS), which integrates voice, facsimile, telex, data, electronic mail and videoconferencing,

b) INTELNET services are confined to data distribution and data collection,

c) nationwide or worldwide satellite-based paging.

Geostationary telecommunications satellites (i.e. they are in stationary [synchronous] orbit relative to the ground) operating currently only reflect data that are beamed up on a different frequency down to another earth station.

However, a new generation of satellites may well work on a different basis: satellites which are not geostationary could transport informations from one point of the orbit to another which would require the storage of data in the space segment over a longer period of time than is necessary for reflecting the data. A German research satellite serving scientists in the Arctic is operating on this basis (like a "postman").

As soon as data are processed in the space segment the classical risks to privacy linked to any form of personal data processing become even greater. The European Commission has realized that communications via satellite tend to evade and bypass national and even EC-legislation. However, the Commission has so far not developed a convincing plan to meet these risks.

2. Positioning and fleet management

Satellites are increasingly being used for purposes of navigation not only by vessels (using the INMARSAT system) but also by trucks and even individuals.

EUTELTRACS is a European satellite based system for land-mobile Communications to manage truck fleets. The position of a driver and his movements with the truck can be checked by a masterstation at any given time. This may save the company time and money and it may even contribute to prevent traffic jams if the masterstation can advise the drivers to take alternative routes which are less crowded.

The Global Positioning System (GPS) was developed by the Pentagon and successfully tested in the Gulf war. It relies on 16 Satellites (21 by the end of 1993) each of which sends the exact time and its position which may be received by anyone using a GPS-receiver which calculates the exact position of the satellite and the receiver. This system allows e.g. a shipping company to locate any of its vessels worldwide and then transmit informations to it via INMARSAT. Pilots and in the near future drivers may use the system together with digital maps to find their way in unknown surroundings.

At the same time it is obvious that an electronic profile of the individual's movements may be created by such a system irrespective of the individual's consent.

3. Telemetry and remote controlling

Satellite-based networks can also be used to monitor and control pipelines, railways, power lines and oil wells. By means of telemetry even the temperature in a refrigerator lorry may be checked and adjusted. At the same time that would mean an intensified surveillance of employees.

4. Remote sensing

Remote sensing is an older (originally military) application of satellites by which natural resources, cloud formations (weather forecast), environmental pollution and even passages of birds can be monitored from the sky.

In 1991 the European Space Agency (ESA) launched a modern Satellite (ERS-1) in order to explore environmental changes. This satellite operates a synthetic aperture radar (SAR) which is able to take pictures of the earth even by night or through a closed cloud cover. This satellite stores certain data until it reaches a position where it can beam them down to the nearest earth station.

Remote sensing satellites used by the allied forces in the Gulf war were able to recognize objects (e.g. tanks) which measured between 1 and 5 meters. lt is very likely that satellite technology developed by the military will be available for civilian use with a certain time lag.

The European Commission plans to control via satellite whether farmers grow less of a certain crop for which they claimed Community subsidies. The technology will soon be available e.g. to read via satellite the headlines of a newspaper which somebody is reading at a bus stop.

5.

The undisputed advantages of satellite technology are accompanied by obvious risks to privacy as soon as the individual comes into focus. Data Protection and Privacy Commissioners should therefore press for international agreements which regulate

– to what extent personal data may be processed in outer space,

– who is the controller of the file, if personal data are stored in the space segment and who is responsible for data safety,

– that special technical measures have to be taken, e.g. encryption services (already in use in military satellites) should be offered for civilian use without additional charges.

The international standardization process for worldwide mobile Communications via satellite still does not sufficiently take data protection into account.

Common Statement

The Data Protection and Privacy Commissioners meeting at their XIVth International Conference in Sydney

– welcome the report of the Working Group on Telecommunications and Media,

– underline the importance of the issues raised in the areas of secrecy of telecommunications and Satellite communications and

– agree to keep a close eye on the technological and legal developments in the field of secrecy of telecommunications in order to protect the privacy of the individual against excessive surveillance.

2006

28. Konferenz, 2. und 3. November 2006, London

Entschließung zum Datenschutz bei Suchmaschinen [1,2]

Heutzutage sind Suchmaschinen der Schlüssel zum „cyberspace“ geworden, um in der Lage zu sein, Informationen im Internet aufzufinden, und damit ein unverzichtbares Werkzeug.

Die steigende Bedeutung von Suchmaschinen für das Auffinden von Informationen im Internet führt zunehmend zu erheblichen Gefährdungen der Privatsphäre der Nutzer solcher Suchmaschinen.

Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. Viele IP-Protokolldaten, besonders wenn sie mit den entsprechenden Daten kombiniert werden, die bei Zugangsdiensteanbietern gespeichert sind, erlauben die Identifikation von Nutzern. Da die Nutzung von Suchmaschinen heute unter den Internet-Nutzern eine gängige Praxis ist, erlauben die bei den Anbietern populärer Suchmaschinen gespeicherten Verkehrsdaten, ein detailliertes Profil von Interessen, Ansichten und Aktivitäten über verschiedene Sektoren hinweg zu erstellen (z. B. Berufsleben, Freizeit, aber auch über besonders sensitive Daten, z. B. politische Ansichten, religiöse Bekenntnisse, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten sind bereits in der Vergangenheit hinsichtlich der Möglichkeit zur Erstellung von Profilen über Bürger besorgt gewesen[3]. Die im Internet verfügbare Technologie macht diese Praxis jetzt in einem gewissen Umfang auf globaler Ebene technisch möglich.

Es ist offensichtlich, dass diese Informationen unter Umständen auf einzelne Personen zurückgeführt werden können. Deswegen sind sie nicht nur für die Betrei-

---

[1] Diese Entschließung bezieht sich nicht auf Suchfunktionen, die von Inhalteanbietern für ihre eigenen Angebote angeboten werden. Für den Zweck dieser Entschließung wird „Suchmaschine“ definiert als ein Service zum Auffinden von Ressourcen im Internet über verschiedene Websites hinweg und basierend auf nutzerdefinierten Suchbegriffen.

[2] Diese Entschließung betrifft nicht Probleme, die durch die Praxis vieler Betreiber von Suchmaschinen aufgeworfen werden, Kopien des Inhalts von Internetseiten einschließlich darauf enthaltener personenbezogener Daten, die dort legal oder illegal veröffentlicht werden, zu speichern und zu veröffentlichen („caching“).

[3] Vgl. z. B. den gemeinsamen Standpunkt zu Datenschutz und Suchmaschinen (zuerst verabschiedet auf der 23. Sitzung in Hongkong SAR, China,15. April 1998, überarbeitet und aktualisiert bei der 39. Sitzung, 6. – 7. April 2006, Washington D. C.) der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation; http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_de.pdf. Vgl. ebenfalls Kapitel 5: „Surfen und Suchen“ des Arbeitsdokuments der Artikel-29-Gruppe „Privatsphäre im Internet“ – ein integrierter EU-Ansatz zum Online-Datenschutz“; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpddocs/2000/wp37de.pdf.

ber von Suchmaschinen selbst von Nutzen, sondern auch für Dritte. So hat zum Beispiel vor kurzem ein Ereignis das Interesse unterstrichen, dass Strafverfolgungsbehörden an diesen Daten haben: Im Frühjahr 2006 forderte das Justizministerium der Vereinigten Staaten von Amerika von Google, Inc. die Herausgabe von Millionen von Suchanfragen für ein Gerichtsverfahren, das unter anderem den Schutz vor der Verbreitung von kinderpornographischen Inhalten im Internet zum Gegenstand hatte. Google weigerte sich, dieser Aufforderung nachzukommen und gewann letztendlich das Verfahren. Im weiteren Verlauf desselben Jahres publizierte AOL eine Liste von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen, die ungefähr 650.000 AOL-Nutzer über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben hatten. Laut Presseberichten konnten daraus einzelne Nutzer auf der Basis des Inhalts ihrer kombinierten Suchanfragen identifiziert werden. Diese Liste war – obwohl sie von AOL umgehend zurückgezogen wurde, als der Fehler dort erkannt worden war – zum Zeitpunkt des Zurückziehens Berichten zufolge bereits vielfach heruntergeladen und neu publiziert, und in durchsuchbarer Form auf einer Anzahl von Websites verfügbar gemacht worden.

Es muss darauf hingewiesen werden, dass nicht nur die Verkehrsdaten, sondern auch der Inhalt von Suchanfragen personenbezogene Informationen darstellen können.

Diese Entwicklung unterstreicht, dass Daten über zurückliegende Suchvorgänge, die von Anbietern von Suchmaschinen gespeichert werden, bereits jetzt in vielen Fällen personenbezogene Daten darstellen können. Insbesondere in Fällen, in denen Anbieter von Suchmaschinen gleichzeitig auch andere Dienste anbieten, die zur einer Identifikation des Einzelnen führen (z. B. E-Mail), können Verkehrs- und Inhaltsdaten über Suchanfragen mit anderen personenbezogenen Informationen kombiniert werden, gewonnen aus diesen anderen Diensten innerhalb derselben Sitzung (z. B. auf der Basis des Vergleichs von IP-Adressen). Der Prozentsatz von Daten über Suchanfragen, die auf Einzelpersonen zurückgeführt werden können, wird vermutlich in der Zukunft weiter ansteigen wegen der Zunahme der Nutzung fester IP-Nummern in Hochgeschwindigkeits-DSL oder anderen Breitbandverbindungen, bei denen die Computer der Nutzer ständig mit dem Netz verbunden sind. Er wird noch weiter ansteigen, sobald die Einführung von Ipv6 abgeschlossen ist.

Empfehlungen

Die Internationale Konferenz fordert die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Richtlinien und Verträgen (z. B. den Richtlinien der Vereinten Nationen und der OECD zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen

zum Datenschutz, und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern:

1. Unter anderem sollten Anbieter von Suchmaschinen ihre Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.

2. Im Hinblick auf die Sensitivität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollten Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und weise anbieten. Insbesondere sollten sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende eines Suchvorgangs sollten keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, für die Erbringung eines Dienstes die notwendig sind, speichern zu lassen (z. B. zur Nutzung für spätere Suchvorgänge).

3. In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, indem die zu treffenden Vorkehrungen bei Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte vereinfacht würden.[4]

28th Conference, 2nd and 3rd November 2006, London

Resolution on Privacy Protection and Search Engines [1,2]

Today, search engines have become the keys to cyberspace in order to be able to find requested information on the Internet, and thus an indispensable tool. The increasing importance of search engines for finding information on the internet increasingly leads to considerable inroads into the privacy of users of search engines.

[4] Für den Zweck dieser Erklärung bedeutet „Dritter" jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle außer der betroffenen Person, dem für die Verarbeitung Verantwortliche, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

[1] This resolution does not address search functions offered by content providers for their own web sites. For the purpose of this resolution, "search engine" shall mean a service for finding resources on the Internet based on user-defined search terms and operating across different web sites.

[2] This resolution does not address the issues raised by the practice of many search engines to store and publish copies of the content of websites, including personal data published on such sites legally or illegally ("caching").

Providers of search engines have the capability to draw up a detailed profile of the interests of their users[3]. Many IP-logs, especially when combined with respective data stored with access providers, allow for the identification of users. Given that the use of search engines is nowadays common practice among netizens, traffic data stored with providers of popular search engines allow for a detailed profile of interests, thoughts and activities across different sectors (for example work, leisure, but also especially sensitive data about e.g. political opinions, religious beliefs, or even sexual preferences).

Data Protection and Privacy Commissioners have been especially concerned about the possibility to draw up profiles of citizens in the past[4]. Now the technology available on the Internet makes this practice, to a certain extent, technically possible on a global basis.

It is clear that this information is potentially personally identifiable. This not only makes it useful to the search engine providers but also to third parties. For example, a recent example highlighted the interest that law enforcement agencies take in this information: In spring 2006, the US Department of Justice had requested from Google, Inc. millions of its users search requests, in a court case inter alia dealing with protection against online child pornography. Google refused to comply and in the end won the case. Later that year, AOL published a list of nearly 20 Million seemingly anonymised search queries about 650.000 AOL users had punched into AOL's search engine over a three-month-period. According to reports in the press, it was possible to identify single users on the basis of the content of their combined search queries. This list, although quickly withdrawn by AOL recognising that it was an error, had by the time of the withdrawal reportedly been downloaded and re-posted many times, and made available in searchable form on a number of websites.

It has to be noted that not only can traffic data constitute personal information, but so can the content of search queries.

These developments underline that search histories stored by providers of search engines now in many cases may constitute personally identifiable data. Specifically, in cases where operators of search engines are also offering other services leading to the identification of an individu al (e.g. e-mail), traffic and content data from searches could be combined with other personally identifiable information

[3] Note that is in some cases done through the use of persistent cookies.

[4] Cf. e.g. the Common Position on Privacy Protection and Search Engines (first adopted at the 23rd Meeting in Hong Kong SAR, China, 15 April 1998; revised and updated at the 39th meeting, 6-7 April 2006, Washington D.C.) of the International Working Group on Data Protection in Telecommunications; http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf. Cf. also CHAPTER 5: SURFING AND SEARCHING of the Article 29 Working Party Working document „Privacy on the Internet" – An integrated EU Approach to On-line Data Protection; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf

derived from those other services during a single session (e.g. based on comparing IP-addresses). The percentage of search history data that can be linked to individuals is likely to further rise in the future due to the uptake of the use of fixed IP numbers in high-speed DSL or other broadband connections where user's computers are "always online". It will further rise once the introduction of IPv6 is completed.

Recommendations

The International Conference calls upon providers of search engines to respect the basic rules of privacy as laid down in national legislation in many countries, as well as in International policy documents and treaties (e.g. the United Nations Guidelines concerning Personal Data Files, the OECD Privacy Guidelines, the CoE Convention 108, the APEC privacy framework, and the data protection and privacy directives of the European Union), and to change their practices accordingly as applicable:

1. Among other things, providers of search engines should inform users upfront in a transparent way about the processing of data in the course of using their services.

2. In view of the sensitivity of the traces users leave when using a search engine, providers of search engines should offer their services in a privacy-friendly manner. More specifically, they shall not record any information about the search that can be linked to users or about the search engine users themselves. After the end of a search session, no data that can be linked to an individual user should be kept stored unless the user has given his explicit, informed consent to have data necessary to provide a service stored (e.g. for use in future searches).

3. In any case, data minimization is key. Such a practice would also be beneficial for the providers of search engines in simplifying arrangements for meeting demands for user-specific information from third parties[5].

[5] For the purpose of this resolution, "third party" shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

2008

30. Konferenz, 15. – 17. Oktober 2008, Straßburg

Entschließung zum Datenschutz in Sozialen Netzwerkdiensten

Soziale Netzwerkdienste[1] haben in den letzten Jahre große Beliebtheit erworben. Diese Dienste bieten ihren Teilnehmern Interaktionsmöglichkeiten auf der Basis von selbst generierten persönlichen Profilen, die in einem noch nie da gewesenen Ausmaß die Veröffentlichung persönlicher Informationen zu den betreffenden Personen (und auch anderen Personen) mit sich bringen. Die sozialen Netzwerkdienste bieten zwar ein neues Spektrum von Möglichkeiten für Kommunikation und den Echtzeit-Austausch von Informationen jeder Art, die Nutzung dieser Dienste kann jedoch auch eine Gefährdung der Privatsphäre ihrer Nutzer – und Anderer – mit sich bringen, denn personenbezogene Daten einzelner Personen werden in bisher unbekannter Weise und Menge öffentlich (und global) zugänglich, einschließlich großer Mengen digitaler Fotos und Videos.

Der Einzelne läuft Gefahr, die Kontrolle über die Nutzung der Daten durch Andere zu verlieren, wenn sie erst einmal im Netzwerk publiziert sind: Während der Community-Bezug sozialer Netzwerke die Vorstellung erweckt, die Veröffentlichung der eigenen persönlichen Daten laufe in etwa auf das Gleiche hinaus, wie früher das Mitteilen von Information unter Freunden von Angesicht zu Angesicht, können Profildaten tatsächlich für alle Teilnehmer einer Community (deren Zahl in die Millionen gehen kann) verfügbar sein.

Derzeit gibt es wenig Schutz dagegen, dass personenbezogene Daten jeder Art aus Profilen kopiert werden – durch andere Mitglieder des Netzwerks oder durch unbefugte netzwerkfremde Dritte – und zum Aufbau von Persönlichkeitsprofilen verwendet werden oder dass die Daten anderweitig wieder veröffentlicht werden. Es kann sehr schwierig – und manchmal unmöglich – sein zu erreichen, dass Daten, wenn sie einmal publiziert sind, wieder vollständig aus dem Internet entfernt werden. Selbst nach ihrer Löschung auf der ursprünglichen Website (z. B. dem sozialen Netzwerk) können Kopien bei Dritten oder bei den Anbietern der sozialen

[1] „Ein sozialer Netzwerkdienst stellt ab auf den Aufbau [...] sozialer Online-Netzwerke für Gruppen von Menschen, die gemeinsame Interessen und Aktivitäten teilen oder daran interessiert sind, die Interessen und Aktivitäten Anderer zu erkunden […]. Die meisten Dienste sind hauptsächlich webbasiert und bieten Nutzern eine Reihe verschiedener Interaktionsmöglichkeiten […]“. Zitat aus Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

Netzwerkdienste verbleiben. Personenbezogene Daten aus Nutzerprofilen können auch außerhalb des Netzwerks bekannt werden, wenn sie von Suchmaschinen indexiert werden. Hinzu kommt, dass manche Anbieter sozialer Netzwerkdienste über Applikationsprogrammierschnittstellen Drittanbietern Nutzerdaten zur Verfügung stellen, die dann unter der Kontrolle dieser Dritten stehen.

Ein Beispiel von Wiederverwendungen, das großes öffentliches Aufsehen erregt hat, ist die Praxis von Personalverantwortlichen, Nutzerprofile von Stellenbewerbern oder Angestellten zu durchsuchen. Presseberichten zufolge gibt bereits heute ein Drittel der Personalverantwortlichen an, bei ihrer Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. um die einzelnen Angaben von Bewerbern zu überprüfen und/oder zu ergänzen.

Profilinformationen und Verkehrsdaten werden von Anbietern sozialer Netzwerkdienste auch zur Weiterleitung zielgerichteter Werbung an ihre Nutzer verwendet.

Sehr wahrscheinlich werden in Zukunft noch weitere unerwartete Verwendungen von Informationen in Nutzerprofilen auftreten.

Zu weiteren, bereits jetzt identifizierten spezifischen Risiken für Datenschutz und Datensicherheit zählen erhöhte Risiken durch Identitätsbetrug, der durch die umfangreiche Verfügbarkeit personenbezogener Daten in Nutzerprofilen begünstigt wird, und durch einemögliche Übernahme von Profilen durch unbefugte Dritte. Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre erinnert daran, dass diese Risiken bereits in dem Dokument „Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten“ („Rom-Memorandum“)[2] der 43. Tagung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommuniktion (3. – 4. März 2008) und in dem ENISA Positionspapier Nr. 1 „Security Issues and Recommendations for Online Social Networks“[3] (Oktober 2007) analysiert wurden.

Die in der Internationalen Konferenz versammelten Datenschutzbeauftragten sind von der Notwendigkeit überzeugt, dass als Erstes eine intensive Informationskampagne unter Beteiligung aller öffentlichen und privaten Interessengruppen – von Regierungsstellen bis zu Bildungseinrichtungen wie Schulen, von Anbietern sozialer Netzwerkdienste bis zu Verbraucher- und Nutzerverbänden, einschließlich der Datenschutzbeauftragten selbst – durchgeführt werden muss, um den vielfältigen mit der Nutzung sozialer Netzwerkdienste verbundenen Gefahren vorzubeugen.

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Empfehlungen

In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdienste:

Nutzer sozialer Netzwerkdienste

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die folgende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdienste sollten sich sorgfältig überlegen, welche persönlichen Daten sie – wenn überhaupt – in einem sozialen Netzwerkprofil publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder mit Bildern konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben. Insbesondere sollten Minderjährige vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen.

Privatpersonen sollten sich überlegen, ob es nicht ratsam wäre, in einem Profil anstelle ihres wirklichen Namens ein Pseudonym zu verwenden. Dabei sollten sie jedoch nicht vergessen, dass auch die Benutzung von Pseudonymen nur einen begrenzten Schutz gewährt, da Dritte in der Lage sein können, ein solches Pseudonym aufzudecken.

2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdienste

Anbieter sozialer Netzwerkdienste tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben.

Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer

Anbieter sozialer Netzwerkdienste sollten ihre Nutzer über die Verarbeitung ihrer personenbezogenen Daten transparent und offen informieren. Es sollte auch aufrichtig und verständlich über mögliche Folgen einer Veröffentlichung persönlicher Daten in einem Profil und über verbleibende Sicherheitsrisiken sowie über gesetzliche Zugriffsrechte Dritter (einschließlich z. B. von Strafverfolgungsbehörden) aufgeklärt werden. Eine solche Aufklärung sollte auch Hinweise dazu enthalten, wie Nutzer mit personenbezogenen Daten von Dritten umgehen sollten, die in ihren Profilen enthalten sind.

3. Nutzerkontrolle

Anbieter sollten die Kontrolle der Nutzer über die Verwendung ihrer Profildaten durch andere Community-Mitglieder weiter verbessern. Sie sollten die Einschränkung der Sichtbarkeit ganzer Profile sowie von in Profilen enthaltenen Daten, und in Community-Suchfunktionen ermöglichen.

Die Anbieter sollten auch eine Kontrolle der Nutzer über die Nutzung von Profil- und Verkehrsdaten, z. B. für zielgerichtete Werbung, ermöglichen. Als ein Minimum sollten eine Opt-out-Möglichkeit für allgemeine Profildaten und eine Opt-in-Möglichkeit für sensible Profildaten (z. B. politische Überzeugungen, sexuelle Orientierung) und Verkehrsdaten geboten werden.

4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofilinformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz des Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt. Diese Einstellungen müssen bei einem sozialen Netzwerkdienst, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer gegen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängigem Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichtigen.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting“) von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Die Anbieter sollten sicherstellten, dass Nutzerdaten von externen Suchmaschinen nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Die Nichtindexierbarkeit von Profilen durch Suchmaschinen sollte als Standard eingestellt sein.

30th Conference, 17th October 2008, Strasbourg

Resolution on Privacy Protection in Social Network Services

Social network services[1] have become very popular in recent years. Among other things, these services offer means for their subscribers to interact based on self-generated personal profiles, which support an unprecedented level of disclosure

[1] “A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others […]. Most services are primarily web based and provide a collection of various ways for users to interact […]”. Quoted from Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

of personal information about the individuals concerned (and others). While social network services offer a new range of opportunities for communication and real-time exchange of all kinds of information, the use of these services can also place the privacy of its users – and others – at risk: Personal data about individuals become publicly (and globally) available in an unprecedented way and quantity, including huge quantities of digital pictures and videos. Individuals face the possible loss of control over how data will be used by others once they are published on the network: While the "community" basis of social networks suggests that publishing one's own personal data would just resemble sharing information with friends as it used to be face-to-face, profile information may in fact be available to an entire subscriber community (numbering in the millions).

Very little protection exists at present against copying any kind of personal data from profiles – by other network members, or by unauthorised third parties from outside the network – and using them for building personal profiles, or re-publishing the data elsewhere. It can be very hard – and sometimes even impossible – to have information thoroughly removed from the Internet once it is published: Even after deletion from the original site (e.g. the social network), copies may rest with third parties or with the social network service providers. Personal data from profiles may also "leak" outside the network when they are indexed by search engines. In addition, some social network service providers make user data available to third parties via application programming interfaces, which are then under control of these third parties.

One example of secondary uses that has gained wide public attention is the practice of company personnel managers crawling user profiles of job applicants or employees: According to press reports, one third of human resources managers already admit to use data from social network services in their work, e.g. to verify and/or complete details of job applicants.

Profile information and traffic data are also used by providers of social network services for delivering targeted marketing messages to their users.

It is very likely that other unexpected uses for the information in user profiles will emerge in the future.

Other specific privacy and security risks already identified include increased risks of identity fraud fostered by the wide availability of personal data in user profiles, and by possible hijacking of profiles by unauthorised third parties. The 30th International Conference of Data Protection and Privacy Commissioners recalls that these risks have already been analyzed in the "Report and Guidance on Privacy in Social Network Services" ("Rome Memorandum")[2] of the 43rd meeting of

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

the International Working Group on Data Protection in Telecommunications (3–4 March 2008), and in the ENISA Position Paper No.1 "Security Issues and Recommendations for Online Social Networks"[3] (October 2007).

The Data Protection and Privacy Commissioners convened at the International Conference are convinced that it is necessary, in the first place, to carry out an in-depth information campaign involving all public and private stakeholders – from governmental authorities to educational institutions, such as schools, from providers of social network services to consumer and user associations, and including the Data Protection and Privacy Commissioners themselves – in order to prevent the multifarious risks associated with the use of social network services.

Recommendations

Given the special nature of the services, and short and long term privacy risks to individuals, the Conference offers the following recommendations to users and providers of social network services:

Users of Social Network Services

Organisations having an interest in the wellbeing of users of social networks – including service providers, governments and Data Protection Authorities – should help educate users to protect their personal data and communicate the following messages.

1. Publication of information

Users of social network services should consider carefully which personal data – if any – they publish in a social network profile. They should keep in mind that they may be confronted with any information or pictures at a later stage, e.g. in a job application situation. In particular, minors should avoid revealing their home address or telephone number.

Individuals should consider the usefulness of using a pseudonym instead of their real name in a profile. However, they should keep in mind that the use of pseudonyms offers limited protection, as third parties may be able to lift such a pseudonym.

2. Privacy of other individuals

Users should also respect the privacy of others. They should be especially careful with publishing personal information about somebody else (including pictures or even tagged pictures) without that other person's consent.

[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Providers of Social Network Services

Providers of social network services have a special responsibility to consider and act in the interests of individuals using social networks. In addition to meeting the requirements of data protection law they should also implement the following recommendations.

1. Privacy regulations and standards

Providers operating in different countries or even globally should respect the privacy standards of the countries where they operate their services. To that end, providers should consult with data protection authorities as necessary.

2. User information

Providers of social network services should inform their users about the processing of their personal data in a transparent and open manner. Candid and intelligible information should also be given about possible consequences of publishing personal data in a profile and about remaining security risks, as well as about possible legal access by third parties (including e.g. law enforcement). Such information should also comprise guidance on how users should handle personal information about others contained in their profiles.

3. User control

Providers should further improve user control over the use of their profile data by community members. They should allow for restriction of visibility of entire profiles, and of data contained in profiles, and in community search functions.

Providers should also allow for user control over secondary use of profile and traffic data; e.g. for targeted marketing purposes. As a minimum, opt-out for general profile data, and opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data should be offered.

4. Privacy-friendly default settings

Furthermore, providers should offer privacy-friendly default settings for user profile information. Default settings play a key role in protecting user privacy: It is known that only a minority of users signing up to a service will make any changes. Such settings must be specifically restrictive when a social network service is directed at minors.

5. Security

Providers should continue to improve and maintain security of their information systems and protect users against fraudulent access to their profile, using rec-

ognised best practices in planning, developing, and running their applications, including independent auditing and certification.

6. Access rights

Providers should grant individuals (regardless of whether they are members of the social network service or not), the right to access and, if necessary, correct all their personal data held by the Provider.

7. Deletion of user profiles

Providers should allow users to easily terminate their membership, delete their profile and any content or information that they have published on the social network.

8. Pseudonymous use of the service

Providers should enable the creation and use of pseudonymous profiles as an option, and encourage the use of that option.

9. Third party access

Providers should take effective measures to prevent spidering and /or bulk downloads (or bulk harvesting) of profile data by third parties

10. Indexibility of user profiles

Providers should ensure that user data can only be crawled by external search engines if a user has given explicit, prior and informed consent. Non-indexibility of profiles by search engines should be a default setting.

2011

33. Konferenz, 1. November 2011, Mexico-Stadt

Entschließung über die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IVp6)

Heute hat sich das Internet zur wichtigsten Technologie für die Übermittlung jeder Art von Kommunikation entwickelt, sei es Sprache, Video oder Daten, und es

wurde zur Grundlage fast aller geschäftlicher Transaktionen und sozialer Interaktionen. Angesichts der drohenden Erschöpfung der Adressen, die vom gegenwärtig genutzten Internet Protokoll Version 4 (IPv4) zur Verfügung gestellt werden, angesichts der anhaltenden enormen weltweiten Nachfrage für Internetadressen und angesichts der Notwendigkeit des Internets zur Unterstützung einer wachsenden Palette neuer Geräte, einschließlich Sensoren und intelligenter Zähler (das „Internet der Dinge"), wurde ein neues Internetprotokoll (IPv6 – IP Version 6) standardisiert, entwickelt und im Laufe der letzten 10 Jahren getestet und muss nun umgesetzt werden.

Obwohl IPv6 im Vergleich zu IPv4 eine Reihe praktischer Vorteile aufweist, können seine Eigenschaften auch zu bestimmten Risiken für den Datenschutz und die Privatsphäre führen, was von der Konfiguration des neuen Protokolls und vor allem von der für die Zuteilung und Zuweisung der IPv6-Adresse gewählten Strategie abhängt. Diese Risiken müssen beim Einsatz der neuen Version des Internetprotokolls angesprochen und kontrolliert werden.

Die Internationale Konferenz gibt folgende Empfehlungen:

- Die Nutzung temporärer und nicht permanenter IPv6-Adressen („dynamische Adressen") muss für jeden Nutzer durch die Beibehaltung der dynamischen Zuweisung von IPv6-Adressen durch ISPs möglich bleiben. Internetzugangsanbieter und Betreiber von Gateways sollte die Nutzung dynamischer IP-Adressen als Standardeinstellung anbieten. Nutzer sollten außerdem in der Lage sein, ihre IP-Adresse während einer Sitzung durch einfaches Verfahren zu ändern. Die Gesetzgeber oder Regulierungsbehörden sollten, soweit erforderlich, es in Erwägung ziehen, entsprechende Verpflichtungen in ihre nationale Rechtsrahmen hinzuzufügen, sofern dies nicht bereits geschehen ist.

- Der Einsatz temporärer und nicht permanenter IPv6-Adressen muss mit den IPv6-Autokonfigurationsfunktionen möglich bleiben, indem alle vorhandenen Möglichkeiten der Pseudorandomisierung der Schnittstellenkennung („Privacy Extensions") genutzt werden. Gerätehersteller – vor allem Hersteller mobiler Geräte – sollten solche Möglichkeiten schnell in ihre Produkte integrieren. Der Einsatz dynamischer Adressen für Endgeräte sollte als Standardfunktion aktiviert werden.

- Als Standardeinstellung sollten Anbieter, Protokolle, Produkte und Dienstleistungen die Nutzung temporärer und nicht permanenter Adressen anbieten.

- Wie jeweils anwendbar, sollten Netzwerke und Applikationen alle Sicherheitsfunktionen von IPv6 (IPSec) in vollem Umfang nutzen, um die Sicherheit, Integrität und Vertraulichkeit zu gewährleisten.

- Immer wenn Standortinformationen für die Nutzung der Dienste auf mobilen Geräten und anderen über IPv6 verbundenen Geräten notwendig ist, sollten solche Informationen z. B. durch Verschlüsselung gegen rechtswidriges Abhören und Missbrauch geschützt werden.

- Alle für die Ausarbeitung und Umsetzung aller weiteren Entwicklungen des IP-Protokolls verantwortlichen Akteure müssen sicherstellen, dass solche Normen und Vorgaben die Datenschutzrechte und Werte von Anfang an vollständig berücksichtigen.

Die Internationale Konferenz begrüßt es, dass die International Working Group on Data Protection in Telecommunications (IWGDPT) derzeit über einen umfassenden Bericht zu diesen Fragen diskutiert. In dem Bericht sollen insbesondere die Auswirkungen einer datenschutzfreundlichen Umsetzung von IPv6 auf dem Gebiet der Strafverfolgung untersucht werden. Die IWGDPT wird gebeten, ihren Bericht unter Berücksichtigung der oben genannten Empfehlungen abzuschließen.

33rd Conference, 1st November 2011, Mexico City

Resolution The Use of Unique Identifiers on the Deployment of Internet Protocol Version 6 (IVp6)

Today the Internet has become the main technology for transporting every kind of communication, whether voice, video or data, and the basis for almost all business transactions and social interactions. Given the imminent exhaustion of the addresses provided by IPv4 Internet Protocol version 4), the protocol currently used for connecting to the Internet, given the continuing enormous demands for Internet addresses in the world and given the need for the Internet to support an increasing array of new devices, including sensors and smart meters (the "Internet of Things"), a new Internet Protocol, (IPv6 – IP version 6) has been standardised, developed and tested during the last 10 years and now needs to be implemented.

Although IPv6 presents a number of practical advantages over IPv4 its characteristics can also lead to specific privacy and security risks, which depend on the configuration of the new protocol and especially on the IPv6 address allocation

and assignment strategy chosen. These risks should be addressed and controlled as the new Internet protocol version is deployed.

The International Conference makes the following recommendations:

- The use of temporary and volatile IPv6 addresses ("dynamic addresses") should remain possible for any user by keeping the dynamic assignment of IPv6 addresses by ISPs. Internet Access Providers and operators of gateways should offer the use of dynamic IP addresses as a default. Users should also be able to change their IP address during a session though a simple procedure. Legislators or regulators, as appropriate, should consider adding respective obligations to their national regulatory frameworks where this is not already the case.

- The use of temporary and volatile IPv6 addresses should remain possible with the IPv6 auto configuration features by using all the existing possibilities of pseudo randomisation of the interface identifier ("privacy extensions"). Equipment manufacturers – and specifically those of mobile devices -should swiftly incorporate such facilities in their products. The use of dynamic addresses for terminal equipment should be activated as a default feature

- By default providers, protocols, products and services should offer the choice to use temporary and volatile addresses.

- As appropriate, networks and applications should fully utilise all the security features of IPv6 (IPSec) to ensure security, integrity and confidentiality.

- Whenever location information is necessary for the use of services on mobile devices and other objects connected via IPv6, such information should be protected, such as by encryption, against unlawful interception and misuse.

- All actors responsible for the elaboration and the implementation of any further evolution of the IP protocol must ensure that any such standards and specifications fully consider privacy and data protection rights and values from the beginning.

The International Conference welcomes that the International Working Group on Data Protection in Telecommunications (IWGDPT) is at present discussing a comprehensive report on these issues. The report should especially examine the effects of a privacy friendly implementation of IPv6 on the area of law enforcement. The IWGDPT is asked to finalize its report in the light of the above mentioned recommendations.

2012

34. Konferenz, 25. und 26. Oktober 2012, Punta del Este, Uruguay

Entschließung zu Cloud Computing

Cloud Computing (CC) gewinnt zunehmend an Interesse, weil es eine größere Wirtschaftlichkeit, weniger Belastung für die Umwelt, einfachere Handhabung, mehr Benutzerfreundlichkeit und viele andere Vorteile verspricht. Aufgrund folgender Tatsachen wirft die Entwicklung von CC viele wichtigen Themen auf, wie z. B. in folgender Hinsicht: Die Technologie befindet sich noch im Entwicklungsstadium, die Datenverarbeitung findet jetzt weltweit statt, und aufgrund der fehlenden Transparenz wird die Durchsetzung von Regelungen zum Schutz der Privatsphäre und der Daten sogar noch erschwert. Dadurch könnten die Risiken, die bei der Datenverarbeitung auftreten, noch erhöht werden, wie Verstöße gegen die Datensicherheit, Verstöße gegen Gesetze und Grundsätze für den Schutz der Privatsphäre und der Daten, und der Missbrauch der in der Cloud gespeicherten Daten.

Die Mitglieder der Internationalen Konferenz und andere Interessengruppen, wie zum Beispiel die International Working Group on Data Protection in Telecommunications (IWGDPT, auch bekannt als „Berlin Group“[1]), hat die mit CC verbundenen datenschutzrechtlichen Probleme untersucht.

Ohne dabei eine von einer bestimmten Gruppe vorgenommene Analyse zu unterstützen, begrüßt die Internationale Konferenz derartige Bemühungen. Um einen Beitrag für die Förderung solcher Bemühungen und zur Vermeidung der mit der Nutzung der Cloud Computing Dienste verbundenen Risiken und zur Förderung der Verantwortlichkeit und der ordnungsgemäßen Geschäftsführung zu leisten, empfiehlt die **Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre** deshalb:

- Im Vergleich mit anderen Arten der Datenverarbeitung darf Cloud Computing nicht zur Absenkung der Datenschutzstandards führen;

- die verantwortlichen Stellen sollen vor der Aufnahme von CC-Projekten die notwendigen Prüfungen der Auswirkungen und Risiken für den Datenschutz durchführen (ggf. durch vertrauenswürdige Dritte)

[1] Siehe z. B. das Arbeitspapier der Gruppe „Cloud Computing – Privacy and data protection issues (Sopot Memorandum)“, Sopot (Polen), 23./24. April 2012; http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

- Die Anbieter von Cloud-Diensten sollen angemessene Transparenz, Sicherheit, Verantwortlichkeit und Vertrauen in CC-Lösungen gewährleisten, insbesondere in Bezug auf Informationen über die Verletzung des Schutzes personenbezogener Daten und in Bezug auf Vertragsklauseln, die gegebenenfalls die Datenportabilität und Datenkontrolle durch Cloud-Nutzer unterstützen. Wenn sie als verantwortliche Stellen handeln, sollen Cloud-Diensteanbieter den Nutzern gegebenenfalls wichtige Informationen über mögliche Auswirkungen auf den Datenschutz und über mit deren Dienste verbundene Risiken zur Verfügung stellen.

- Es sollen weitere Bemühungen im Bereich der Forschung, der Zertifizierung durch Dritte, Standardisierung, „Privacy by Design"-Technologien und anderen, damit verbundenen Systemen unternommen werden, um das gewünschte Maß an Vertrauen in CC zu erreichen. Um den Datenschutz gründlich und wirksam in Cloud Computing einzubauen, sollten schon im Anfangsstadium angemessene Maßnahmen in die Architektur von IT-Systemen und Geschäftsabläufen einbezogen werden (Privacy by Design).

- Die Gesetzgeber sollen die Angemessenheit und Interoperabilität der bestehenden Rechtsrahmen zur Erleichterung grenzüberschreitender Datenübermittlungen überprüfen, und sie sollten zusätzliche notwendige Maßnahmen zum Datenschutz im Bereich CC in Erwägung ziehen.

- Die Datenschutzbehörden sollen den verantwortlichen Stellen, Anbietern von Cloud-Diensten und Gesetzgebern weiterhin mit Informationen zu Fragen hinsichtlich des Schutzes der Privatsphäre und personenbezogener Daten zur Verfügung stehen.

Alle Interessengruppen – Anbieter, Kunden von CC und auch Regulierungsbehörden – sollten zusammenarbeiten, um ein hohes Datenschutzniveau und eine hohe IT-Sicherheit zu gewährleisten.

34th Conference, 26th October 2012, Punta del Este, Uruguay

Resolution on Cloud Computing

Cloud Computing (CC) is attracting increasing interest due to promises of greater economic efficiency, lower environmental impact, simpler operation, increased user-friendliness and a number of other benefits. However, the evolution of CC raises a number of important issues relating to, for example, the fact that the technology is still developing, data processing has become global, and lack of

transparency is making it more difficult to enforce privacy and data protection rules. These issues may magnify certain risks inherent in data processing, such as breaches of information security, violation of laws and principles for privacy and data protection, and misuse of data stored in the cloud.

Members of the International Conference and other stakeholders, including, for example, the International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group")[1], have begun to consider data protection and privacy issues relating to CC.

Without endorsing any particular group's analysis, the International Conference welcomes such efforts. Therefore, to further encourage such efforts and to helpreduce risks associated with the use of cloud computing services and to promote accountability and proper governance,

the 34th International Conference of Data Protection and Privacy Commissioners recommends that:

- Cloud computing should not lead to a lowering of privacy and data protection standards as compared with other forms of data processing;

- Data controllers carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on CC projects;

- Cloud service providers ensure that they provide appropriate transparency, security, accountability and trust in CC solutions in particular regarding information on data breaches and contractual clauses that promote, where appropriate, data portability and data control by cloud users; cloud service providers, when they are acting as data controllers, make available to users, where appropriate, relevant information about potential privacy impacts and risks related to the use of their services.

- Further efforts be put into research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC; to build privacy thoroughly and effectively into cloudcomputing adequate measures should be embedded into the architecture of IT systems and business processes at an early stage (privacy by design);

- Legislators assess the adequacy and interoperability of existing legal frameworks to facilitate cross-border transfer of data and consider additional necessary privacy safeguards in the era of CC, and

[1] See, e.g., the Group's Working paper "Cloud Computing – Privacy and data protection issues (Sopot Memorandum)", Sopot (Poland), 23./24. April 2012; http://www.datenschutz- berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

- Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues.

All stakeholders – providers and customers of CC as well as regulators – should cooperate in order to ensure a high level of privacy and data protection and IT security.

2013

35. Konferenz, 23.–26. September 2013, Warschau

Entschließung „Verankerung des Datenschutzes und des Schutzes der Privatsphäre im internationalen Recht“

Die Konferenz ruft in Erinnerung, dass sie:

– bereits auf ihrer 27. Sitzung in Montreux die Vereinten Nationen aufgefordert hat, ein verbindliches Rechtsinstrument vorzubereiten, in dem die Rechte auf Datenschutz und dem Schutz der Privatsphäre als einklagbare Menschenrechte klar und detailliert geregelt sind,

– auf ihrer 28. Sitzung in Montreal die Verbesserung der internationalen Zusammenarbeit beim Datenschutz und dem Schutz der Privatsphäre gefordert hat,

– auf ihrer 30. Sitzung in Straßburg eine Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung eines gemeinsamen Vorschlags zur Abfassung internationaler Standards zum Schutz der Privatsphäre und zum Schutz der personenbezogenen Daten verabschiedet hat,

– auf ihrer 31. Sitzung in Madrid internationale Standards zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre angenommen hat (Erklärung von Madrid),

– auf ihrer 32. Sitzung in Jerusalem die Regierungen zur Einberufung einer Regierungskonferenz aufgefordert hat, um ein verbindliches internationales Übereinkommen zum Schutz der Privatsphäre und der Daten zu erarbeiten, mit dem die Erklärung von Madrid umgesetzt wird,

und sie erinnert an die Wichtigkeit bestehender Instrumente im internationalen Recht, die Regelungen und Standards für den Schutz personenbezogener Daten vorsehen, insbesondere das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108).

Die 35. Internationale Konferenz stellt fest,

dass eine dringende Notwendigkeit für eine verbindliche internationale Vereinbarung zum Datenschutz besteht, das die Menschenrechte durch den Schutz der Privatsphäre, der personenbezogenen Daten und der Integrität von Netzwerken gewährleistet und die Transparenz der Datenverarbeitung erhöht, und dabei ein ausgewogenes Verhältnis im Hinblick auf Sicherheit, wirtschaftliche Interessen und freie Meinungsäußerung wahrt.

und beschließt

die Regierungen auffordern, sich für die Verabschiedung eines Zusatzprotokolls zu Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR) einzusetzen, das auf den Standards, die von der Internationalen Konferenz entwickelt und gebilligt wurden, und auf den Bestimmungen im allgemeinen Kommentar Nr. 16 zum Pakt basieren sollte, um weltweit gültige Standards für den Datenschutz und den Schutz der Privatsphäre zu schaffen, die im Einklang mit der Rechtsstaatlichkeit stehen.

Die Federal Trade Commission der USA enthielt sich bei der Abstimmung über diese Entschließung.

Erläuternde Anmerkungen

Die 35. Internationale Konferenz stellt fest, dass der im Jahre 1966 von der Generalversammlung der Vereinten Nationen angenommene und von 167 Staaten ratifizierte IPBPR bereits einen rechtlichen Rahmen für den Schutz der Privatsphäre bietet. Artikel 17 des IPBPR lautet:

1. Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.

2. Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Darüber hinaus bietet der allgemeine Kommentar Nr. 16 des IPBPR weitere Erläuterungen zu den datenschutzrechtlichen Bestimmungen unter Artikel 17. Dort heißt es, unter anderem, dass,

- die Erhebung und Speicherung personenbezogener Daten auf Computern, in Datenbanken oder anderen Geräten, sei es von öffentlichen oder privaten Stellen, gesetzlich geregelt werden müssen;
- die Staaten wirksame Maßnahmen ergreifen müssen um sicherzustellen, dass Informationen über das Privatleben einer Person nicht in die Hände von Personen gelangen, die nicht gesetzlich zum Erhalt, zur Verarbeitung und zur Nutzung dieser Informationen berechtigt sind;
- Nutzungen dieser Informationen zu Zwecken, die mit dem Pakt nicht vereinbar sind, verhindert werden müssen;
- die Einzelnen das Recht haben sollten, zu bestimmen, welche Informationen über sie gespeichert werden und für welche Zwecke, sowie das Recht, einen Antrag auf Berichtigung oder Löschung fehlerhafter Informationen zu stellen;
- jeder „Eingriff" in diese Rechte nur auf einer gesetzlichen Grundlage erfolgen darf, die mit dem Pakt im Einklang steht.

Diese Forderungen werden durch die Verpflichtung der speichernden Stelle zur Transparenz bei der Datenverarbeitung ergänzt, insbesondere in Bezug auf die Bereitstellung von Informationen, Korrektur und Löschung als wesentliche Datenschutzgrundsätze.

35th Conference, 23 – 26 September 2013, Warsaw

Resolution on anchoring data protection and the protection of privacy in international law

Recalling that

– the 27th Conference in Montreux appealed to the United Nations to prepare a legally binding instrument which clearly and in detail sets out the rights to data protection and privacy as enforceable human rights,

– the 28th Conference in Montréal called for the improvement of international cooperation with respect to data protection and the protection of privacy,

– the 30th Conference in Strasbourg adopted a resolution on the urgent need for protecting privacy in a borderless world and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection,

– the 31st Conference in Madrid adopted International Standards on the Protection of Data and Privacy (the Madrid Declaration),

– the 32nd Conference in Jerusalem urged governments to organise an intergovernmental conference with a view to developing a binding international agreement on privacy and data protection giving effect to the Madrid Declaration,

and recalling the importance of existing instruments in international law that provide rules and standards for the protection of personal data, in particular the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

The 35th International Conference observes

that there is a pressing need for a binding international agreement on data protection that safeguards human rights by protecting privacy, personal data and the integrity of networks and enhances the transparency of data processing while striking the right balance in respect of security economic interests and freedom of expression,

and **resolves**

to call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law.

EXPLANATORY NOTE

The 35th International Conference notes that the ICCPR, adopted by the General Assembly of the United Nations in 1966 and ratified by 167 states, already provides a legal framework for privacy protection. Article 17 of the ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

In addition, General Comment No. 16 to the ICCPR provides further specification on data protection requirements under Article 17. It states, among other things, that

- the collection and storage of personal information on computers, in data bases or other devices, whether by public or private bodies, must be regulated by law;
- states must take effective measures to ensure that information concerning a person‘s private life does not reach the hands of persons who are not authorized by law to receive, process and use it;
- uses of this information for purposes incompatible with the Covenant must be prevented;
- individuals should have the right to determine what information is being held about them and for what purposes and to request rectification or elimination of incorrect information;
- any “interference” with these rights must only take place on the basis of law which must comply with the Covenant.

These requirements are supplemented by the storing body’s duty of transparency with regard to data processing, in particular as regards the provision of information, rectification and elimination as vital data protection principles.

Entschließung zu Webtracking und Datenschutz

Web Tracking ermöglicht den Organisationen die Überwachung fast jeden einzelnen Aspekts des Nutzerverhaltens im Internet. Die Art von Information, die durch Tracking erhoben werden kann, (z. B. IP-Adressen, Gerätekennungen, etc.), kann zur Identifizierung eines bestimmten Betroffenen führen. Diese Fähigkeit eröffnet den Organisationen die Möglichkeit zur Entwicklung eines umfangreichen Profils über die Online-Aktivitäten eines identifizierbaren Betroffenen über einen längeren Zeitraum.

Daten über Nutzeraktivitäten, die von einem Computer oder einem anderen Gerät (z. B. einem Smartphone) während der Nutzung verschiedener Dienste der Informationsgesellschaft im Internet erhoben werden, werden zunehmend von unter-

schiedlichen Akteuren für verschiedene Zwecke kombiniert, korreliert und analysiert, die sich von karitativen bis zu kommerziellen Zwecken der unterschiedlichen Akteure erstrecken, die solche Dienstleistungen oder Teile davon anbieten. Die erzeugten Interessenprofile (oder „Nutzerprofile“) können mit Daten der „offline-Welt“ über fast jeden Aspekt des Privatlebens, einschließlich finanzieller Informationen wie auch Informationen, beispielsweise über Freizeitinteressen, gesundheitliche Probleme, politische Ansichten und/oder religiöse Meinungen angereichert werden.

Wir erkennen an, dass Tracking den Verbrauchern einige Vorteile wie Netzwerk-Management, Sicherheit und Betrugsprävention bietet und die Entwicklung neuer Produkte und Dienstleistungen erleichtern kann. Dennoch stellt Tracking ein ernsthaftes Risiko für die Privatsphäre der Bürger in einer Informationsgesellschaft dar, denn es droht, die wichtigsten datenschutzrechtlichen Grundsätze der Transparenz, Zweckbindung und individuelle Kontrolle zu untergraben.

Als Konsequenz hieraus sollten alle Beteiligten, einschließlich Regierungen, internationalen Organisationen und Anbietern von Informationsdiensten den Schutz der Privatsphäre beim Design, der Bereitstellung und Nutzung von Diensten der Informationsgesellschaft an die erste Stelle setzen.

Die Internationale Konferenz der Beauftragten für Datenschutz und Privatsphäre fordert daher alle Beteiligten auf, soweit es relevant und angebracht ist, folgendes zu unternehmen:

- Beachtung des Grundsatzes der Zweckbindung;
- Benachrichtigung und Kontrolle über die Verwendung von Tracking-Elementen, einschließlich Geräte- und Browser Fingerprinting;
- Verzicht auf die Nutzung unsichtbarer Tracking-Elemente zu anderen Zwecken als für Sicherheit / Betrugsaufdeckung oder Netzwerk-Managment;
- Verzicht auf die Ableitung eines Satzes an Informationselementen (Fingerabdrücke) für die alleinige Identifizierung und Verfolgung von Nutzern zu anderen Zwecken als für Sicherheit / Betrugsprävention oder Netzwerk-Management;
- Gewährleistung angemessener Transparenz über alle Arten von Web-Tracking-Verfahren, damit die Verbraucher eine informierte Wahl treffen können;
- Angebot einfach zu bedienender Werkzeuge, um den Nutzern angemessene Kontrolle über die Erhebung und Nutzung ihrer personenbezogenen Daten zu ermöglichen;
- Vermeidung des Trackings von Kindern und des Trackings auf an Kinder gerichtete Webseiten;

- Beachtung des Grundsatzes des Privacy-by-Design und Durchführung einer Datenschutz-Folgenabschätzung zu Beginn neuer Projekte;

- Verwendung von Techniken, die die Auswirkungen auf die Privatsphäre mindern, wie Anonymisierung / Pseudonymisierung;

- Förderung technischer Standards für eine bessere Nutzerkontrolle (z. B. ein wirksamer Do-Not-Track Standard).

Die Datenschutzbeauftragte der Republik Slowenien und die Französische Datenschutzbehörde enthielten sich bei der Abstimmung über diese Entschließung.

Resolution on webtracking and privacy

Web tracking allows organisations to monitor almost every single aspect of user behaviour on the Web. The type of information that can be collected through tracking (e.g., IP addresses, device identifiers, etc.) can lead to the identification of a particular data subject. This capability creates the potential for organisations to develop a rich profile of an identifiable data subject's online activities over extended periods.

Data on user activity, collected from a computer or other device (e.g., a smart phone) while using various services of the information society on the Internet, are increasingly combined, correlated and analysed by different actors for various purposes ranging from charitable to commercial purposes of the different actors offering such services or parts thereof. Generated interest profiles (or "user profiles") can be enriched with data from the "offline world" on almost every aspect of private life, including financial information as well as information on, for instance, leisure interests, health concerns, political views and/or religious opinions.

We recognise that tracking offers some consumer benefits, such as network management, security, and fraud prevention, and may facilitate the development of new products and services. Nevertheless tracking poses serious privacy risks for citizens in an information society, threatening to erode the core privacy principles of transparency, purpose limitation and individual control.

Consequently, all stakeholders, including governments, international organisations and providers of information services should prioritise the protection of privacy in the design, provision and use of services of the information society.

The International Conference of Data Protection and Privacy Commissioners therefore calls on all stakeholders to do the following where relevant and appropriate:

- observe the principle of purpose limitation;
- provide notice and control over the use of tracking elements, including device and browser fingerprinting;
- refrain from the use of invisible tracking elements for purposes other than security/fraud detection or network management
- refrain from deriving a set of information elements (fingerprint) in order to uniquely identify and track users for purposes other than security/fraud prevention or network management;
- ensure adequate transparency about all types of web tracking practices to enable informed consumer choices;
- offer easy to use tools to allow users appropriate control over the collection and use of their personal data;
- avoid tracking children and tracking on websites aimed at children absent verifiable parental consent;
- respect the principle of privacy-by-design and conduct a privacy impact assessment at the start of new projects;
- use techniques that reduce the privacy impact, such as anonymisation / pseudonymisation;
- promote technical standards for better user control (e.g., an effective Do-Not-Track standard).

C. Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation: Gemeinsame Standpunkte, Memoranden und Arbeitspapiere / International Working Group on Data Protection in Telecommunications: Common Positions, Memoranda and Working Papers

1990

Memorandum
vom 12.11.1990 zum Vorschlag der EG-Kommission

für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen

auf der Grundlage der Beratungen der Arbeitsgruppe am 12. November 1990 in Berlin

Vor dem Hintergrund des Beschlusses der 12. Internationalen Konferenz der Datenschutzbeauftragten vom 19. September 1990 zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens begrüßen die Datenschutzbeauftragten der EG-Mitgliedstaaten die Initiative der EG-Kommission, einen Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen vorzuschlagen. Ein gemeinschaftsweiter Schutz von Teilnehmerdaten und eine Beschränkung elektronischer Spuren auf das unerläßliche Minimum sind von entscheidender Bedeutung und können effektiv nur durch Gemeinschaftsrecht gewährleistet werden. Die Datenschutzbeauftragten der EG-Mitgliedstaaten unterstützen deshalb grundsätzlich den Vorschlag der Kommission. Sie regen allerdings einzelne Veränderungen des Entwurfs an, um den Datenschutz auf europäischer Ebene zu verbessern.

Während und nach der Einführung von ISDN werden analoge Netze noch für eine beträchtliche Zeit parallel zum ISDN weiterbestehen. Es ist deshalb von entscheidender Bedeutung, daß die Regelungen der Richtlinien umgesetzt werden, bevor analoge Netze aufhören zu bestehen. Art. 2 Abs. 2 des gegenwärtigen Entwurfes sollte insoweit um eine Klarstellung ergänzt werden, damit Umgehungsversuche vereitelt werden. Ohne diese Klarstellung könnte man sich

auf den Standpunkt stellen, daß die Vorschriften der Richtlinie in solchen Mitgliedstaaten, die ISDN oder öffentliche digitale Mobilfunknetze bereits eingeführt haben, nicht auf Dienste in weiterbestehenden analogen Netzen anwendbar sind.

Der Entwurf verwendet die Begriffe „Telekommunikationsgeräte" (Art. 1 Abs. 1) und „Anbieter der Dienste" (Art. 16 Abs. 2), ohne sie zu definieren. Dies ist jedoch notwendig, um den genauen Anwendungsbereich der Richtlinie festzustellen. Es ist z. B. unklar, ob und in welchem Umfang Anbieter von Mailbox-Diensten von der Richtlinie erfaßt werden. Private Dienste-Anbieter sollten erfaßt werden, wenn sie für die Öffentlichkeit Telekommunikationsdienste erbringen unabhängig davon, ob die Mitgliedstaaten ihnen „besondere oder ausschließliche Rechte" gewährt haben. In bestimmten Mitgliedstaaten (z. B. in der Bundesrepublik) besteht keine Notwendigkeit, die Gewährung solcher „besonderen oder ausschließlichen Rechte" zu beantragen, um auf privater Basis derartige Dienste erbringen zu können. Die Begriffsbestimmungen in Art. 3 des Entwurfs sollten dementsprechend geändert werden.

Die 12. Internationale Konferenz der Datenschutzbeauftragten hat betont, daß jeder Teilnehmer das Recht hat, gebührenfrei und ohne Begründung den Eintrag seiner Daten in ein Teilnehmerverzeichnis auszuschließen. Dieses Recht sollte in einem gesonderten (neuen) Artikel des Richtlinienentwurfs bekräftigt werden. Dieser könnte wie folgt lauten:

„Teilnehmerverzeichnisse

(1) Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

(2) Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr Geschlecht und ihren Wohnort auszuschließen. Dies schließt die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus."

Art. 4 (1) des Entwurfs müßte entsprechend modifiziert werden.

In Art. 5 Abs. 2 des Entwurfs sollte eine klare Unterscheidung zwischen der Verantwortung der Telekommunikationsorganisationen einerseits und der Dienste-Anbieter andererseits aufgenommen werden. Sie könnte wie folgt formuliert werden:

„(2) Die Inhalte der übertragenen Information dürfen von der Telekommunikationsorganisation nur im Auftrag von Dienste-Anbietern insoweit gespei-

chert werden, als diese vertraglich zur Speicherung von Inhaltsdaten verpflichtet sind, es sei denn, dies ist aufgrund von Verpflichtungen erforderlich, die in den Mitgliedstaaten dem Gemeinschaftsrecht entsprechend gesetzlich vorgeschrieben sind."

In Art. 7 Abs. 1 sollte das Wort „grundsätzlich" gestrichen und der Satz entsprechend umgestellt werden. Folgender neuer Satz 2 sollte diesem Absatz angefügt werden:

„Jeder Mitgliedsstaat erläßt Vorschriften für strafrechtliche Sanktionen, um die Vertraulichkeit personenbezogener Daten, die bei der Bereitstellung von Telekommunikationsnetzen und -diensten verarbeitet werden, zu gewährleisten."

In Art. 7 Abs. 2 (Sätze 1 und 3) sollte das Wort „schriftlich", das bereits in der deutschen Entwurfsfassung enthalten ist, auch in die französischen und englischen Fassungen übernommen werden.

In Art. 8 Abs. 1 sollten die Worte „dem Stand der Technik entsprechenden, angemessenen Schutz" ersetzt werden durch die Worte „wirksamen, hohen Standard des Schutzes". In Abs. 2 desselben Artikels können die Worte „der Verletzung der" ersetzt werden durch „für die".

Die 11. Internationale Konferenz hat anonyme Zahlverfahren für bestimmte Telekommunikationsdienste wie das Telefon und Datenübertragungsdienste gefordert, um die Speicherung von Gebührendaten zu begrenzen. Dies sollte in der Formulierung des Artikels 9 des Richtlinienentwurfs zum Ausdruck kommen.

Art. 12 Abs. 3 sollte wie folgt umformuliert werden:

„(3) Bei Verbindungen zwischen einem Teilnehmer, der mittels analoger Technik an eine Vermittlungsstelle angeschlossen ist, und einem Teilnehmer, der mittels digitaler Technik an eine Vermittlungsstelle angeschlossen ist, muß ersterer über die Möglichkeit informiert werden, daß seine Rufnummer angezeigt wird. Die Telekommunikationsorganisation muß die vorherige schriftliche Einwilligung dieses Teilnehmers einholen, bevor sie die Möglichkeit der Rufnummernanzeige schafft. Dieser Teilnehmer muß ebenfalls die Möglichkeit haben, die Rufnummernanzeige von Fall zu Fall auszuschließen." (letzter Satz unverändert)

Die 12. Internationale Konferenz hat betont, daß die Möglichkeit der Unterdrückung der Rufnummernanzeige von Fall zu Fall in gleicher Weise bestehen muß, wenn grenzüberschreitende Telefongespräche geführt werden. Deshalb sollte ein neuer Art. 12 Abs. 4 in den Entwurf aufgenommen werden:

„(4) Wenn ein Teilnehmer die Unterdrückung der Rufnummernanzeige bei Auslandsgesprächen mit Teilnehmern in solchen Mitgliedstaaten beantragt hat, in denen bisher keine den Absätzen 1 bis 3 dieses Artikels entsprechenden Maßnahmen ergriffen worden sind, so darf die Verbindung nur ohne Rufnummernanzeige beim angerufenen Teilnehmer hergestellt werden."

Bisher enthält der Entwurf lediglich in Art. 13 Abs. 3 eine Regelung der gemeinschaftsweiten Aufhebung der Unterdrückung der Rufnummeranzeige in bestimmten Fällen.

Art. 16 Abs. 1 des Entwurfs sollte wie folgt präzisiert werden:

„Die Telekommunikationsorganisation darf die Telefonnummer sowie sonstige personenbezogene Daten des Teilnehmers, insbesondere Art und Länge seiner Bestellungen über einen Teleshopping-Dienst oder die über einen Videotext-Dienst angeforderten Informationen, nur im Auftrag eines Dienste-Anbieters und nur insoweit speichern, als dies unbedingt zur Erbringung des Dienstes erforderlich ist. Diese Daten dürfen nur vom Dienste-Anbieter und ausschließlich für die vom Teilnehmer gestatteten Zwecke verwendet werden."

Angesichts der wachsenden Bedeutung der Direktwerbung über Telefon und Telefax z. B. durch automatische Wählvorrichtungen sollte Art. 17 des Entwurfs in der Weise modifiziert werden, daß jeder Teilnehmer das Recht hat, keine Telefonanrufe oder Telekopien zu Werbezwecken oder mit Angeboten von Gütern und Dienstleistungen zu erhalten, wenn er dem nicht zuvor schriftlich zugestimmt hat.

In Art. 17 Abs. 2 sollte deutlicher gemacht werden, daß nur der Dienste-Anbieter dafür verantwortlich ist, die notwendigen Maßnahmen dafür zu treffen, daß die Übermittlung von aufgedrängten Informationen (insbesondere Werbung) an den Teilnehmer unterbleibt, und eine Liste mit schriftlichen Einverständniserklärungen zu führen. Anderenfalls würde die Telekommunikationsorganisation das Fernmeldegeheimnis im Sinne des Art. 7 Abs. 1 verletzen.

Memorandum
of 12th November 1990 on the Proposal of the EC Commission

for a Council Directive concerning the protection of personal data and privacy in the integrated services digital network (ISDN) and public digital mobile networks

based on the discussions of the Working Group on 12 November 1990 in Berlin

In view of the resolution on problems related to public telecommunications networks and cable television adopted by the XIIth International Conference of Data Protection Commissioners on 19 September 1990 the Data Protection Commissioners of EEC Member States welcome the initiative taken by the EC Commission to propose a Draft Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks. A Community-wide protection of subscribers' data and a reduction of electronic traces to the necessary minimum are essential and can only be ensured effectively by community legislation. The Data Protection Commissioners of EC Member States therefore support in principle the proposal put forward by the Commission. They suggest, however, specific amendments in the Draft to improve data protection on the European level.

During and after the introduction of ISDN analogue networks will continue to exist parallel to ISDN for quite some time. It is therefore essential that the provisions of the Directive should be implemented before analogue networks have ceased to exist. Art. 2 par. 2 of the present Draft needs clarification in this respect in order to prevent circumvention. Without this clarification one could argue that the provisions of the Directive do not apply to services based on analogue networks in Member States which have implemented ISDN or public digital mobile networks.

The Draft refers to "telecommunications equipment" (Art. 1 par. 1) and "service provider" (Art. 16 par. 2) without defining these terms. This is however necessary in order to determine the exact scope of the Directive. It is e. g. not clear whether and to what extent providers of mailbox services will be covered by the Directive. Private service providers should be covered if they provide services to the public irrespective of "special or exclusive rights" granted to them. In certain Member States (e. g. the Federal Republic) there is no need to apply for special or exclusive rights in order to provide services on a private basis. The definitions in Art. 3 of the Draft should be amended accordingly.

The XIIth International Conference of Data Protection Commissioners has stressed that subscribers have the right, free of charge and without having to give reasons, to have no personal data included in a directory. Therefore a new Article should be included in the Draft dealing with directories in particular. This Article could read as follows:

„Directories

(1) Subscribers have the right, free of charge and without having to give reasons, to have no personal data included in a directory.

(2) Personal data contained in a directory should be limited to such as are strictly necessary to identify reasonably a particular subscriber. He/ she also has the right not to indicate his/ her sex. This does not exclude the publication of additional data at the request of the subscriber."

Art. 4 par. 1 of the Draft should be amended accordingly.

Art. 5 par. 2 of the Draft should be clarified in order to keep a clear distinction between the responsibilities of telecommunications organizations and service providers in the following way:

„(2) The contents of the information may be stored by the telecommunications organization only on behalf of service providers inasmuch as they are under a contractual obligation to store content data, except where required by obligations imposed by the law of the Member State, in conformity with Community law."

In Art. 7 par. 1 the words „In principle," should be deleted. The following new second sentence should be added to this provision:

„Each Member State shall make provision for penal sanctions in order to ensure confidentiality of personal data processed in connection with telecommunication networks and services."

In Art. 7 par. 2 (first and third sentence) the word „written" should be inserted before consent in the French and English version of the Draft. It is already contained in the German version.

In Art. 8 par. 1 the words „adequate, state-of-the-art" should be replaced by „effective, high-standard". In par. 2 of the same article the words „of a breach of" can be replaced by „to".

The XIth International Conference has called for anonymous payment procedures for certain telecommunications services such as telephone and data transfer services in order to limit the storage of billing data. This should be reflected in the wording of Art. 9 of the Draft Directive.

Art. 12 par. 3 should be redrafted in the following way:

„(3) With regard to communications between a subscriber linked to an exchange by an analogue connection and subscribers linked to an exchange by a digital connection, the former subscriber is to be informed of the possibility of the identification of his/ her telephone number. The telecommunications organization is to obtain this subscriber's prior written Consent before it starts

operating the possibility of identification. This subscriber must also have the possibility to eliminate the identification on a case-by-case basis.“ (Last phrase unchanged)

The XIIth International Conference stressed that the possibility to suppress the calling line identification on a call-by-call basis shall be equally guaranteed when operating international calls. Therefore a new Art. 12 par. 4 should be included in the Draft:

„(4) In case a subscriber has asked to eliminate the identification of his/her telephone number when making a call to a State where the provisions of Art. 12 pars. 1–3 have not been implemented the connection shall be established without identifying the calling subscriber‘s telephone number.“

The present Draft only provides for the operation of the override function on a Community- wide basis (Art. 13 par. 3).

Art. 16 par. 1 of the Draft should be clarified as follows:

„The telecommunications organization may only store the telephone number as well as other personal data of the subscriber, in particular concerning the quantity and nature of his/ her orders when using a teleshopping service or concerning the information requested via a videotex service, on behalf of a service provider to the extent strictly necessary to supply the service. These data may only be used by the service provider for purposes authorized by this subscriber.“

Bearing in mind the growing importance of direct marketing by telephone or telefax e. g. via automatic calling devices Art. 17 should be redrafted in such a way that every subscriber has the right not to receive calls for advertising purposes or for the purpose of offering the supply or provision of goods and services without his/her prior written consent.

In Art. 17 par. 2 it should be made clearer that only the service provider concerned is responsible to take the steps necessary to terminate the transmission of unsolicited messages to the subscribers and to keep a list of written consent declarations. Otherwise there was bound to be a breach of confidentiality in the sense of Art. 7 par. 1 by the telecommunications organization.

1991

Stellungnahme
vom 6. Februar 1991 zum Artikel 19 des Vorschlags der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

Die Arbeitsgruppe Telekommunikation und Medien der Internationalen Konferenz der Datenschutzbeauftragten erörterte auch Artikel 19 des Entwurfs einer Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (COM[90]314 final-SYN 287) und die unterschiedlichen nationalen Regelungen des Verhältnisses zwischen Datenschutz und Pressefreiheit. Die Arbeitsgruppe schlägt keine bestimmte Änderung des Entwurfstexts (Art. 19) vor, regt aber an, seine Formulierung erneut zu überprüfen, um eine präzisere Abgrenzung der zulässigen Ausnahmen zu erreichen. Insbesondere sollten die folgenden Punkte berücksichtigt werden:

Das Medienprivileg sollte sich nur auf Datensammlungen für journalistische Zwecke erstrecken;

Das Privileg sollte auch für zu journalistischen Zwecken gesammelte Daten nicht gelten, wenn sie Dritten für andere Zwecke (z. B. Werbezwecke) zugänglich gemacht werden;

Wenn ein Recht zur Veröffentlichung einer Gegendarstellung oder Richtigstellung besteht, sollte ein Hinweis auf diese Gegendarstellung oder Richtigstellung zusammen mit dem ursprünglichen Text gespeichert werden;

Das Recht des Einzelnen auf Zugang zu veröffentlichten Informationen, die über ihn gespeichert sind, sollte erhalten bleiben (außer wenn dies zur Bekanntgabe der Informationsquelle führen würde);

Die Existenz des Medienprivilegs darf nicht zu einem völligen Fehlen der Datenschutzkontrolle führen. Falls personenbezogene Daten über Abonnenten einer Zeitschrift oder Nutzer eines Informationsdienstes verarbeitet werden, sollte sich das Medienprivileg nicht auf solche Daten erstrecken.

Statement
of 6th February 1991 on Article 19 of the Proposal of the EC Commission for a general Data Protection Directive

The Working Group on Telecommunications and Media of the International Data Commissioners Conference also discussed Article 19 of the Draft Directive concerning the protection of individuals in relation to the processing of personal data (COM[90]314 final-SYS 287) and the different national approaches to data protection and freedom of the press. The group does not propose any particular new formulation of the text of article 19, but suggests that it should be reexamined with a view to a more precise limitation on the derogation permitted. In particular, the following points need to be considered:

that the media privilege should extend only to data collected for journalistic purposes;

that the privilege should not extend to such data if they are made available to third parties for other purposes (for example marketing);

that if there is a right to have a counter-statement or a correction published, a reference to this statement or correction should appear with the original text;

that the right of access by an individual to published information stored about him or her (except for revealing the identity of the source) should be retained;

that the existence of a privilege for the media should not mean a complete absence of data protection control.

In the case that personal data are collected on subscribers to a journal or users of an information service, any media privilege should not apply to such data.

1996

20. Sitzung, 15. und 16. April 1996, Berlin

Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet („Budapest – Berlin Memorandum“)

Zusammenfassung

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz von Benutzern des Internet gegenwärtig unzureichend ist.

In diesem Dokument werden zehn Prinzipien zur Verbesserung des Datenschutzes im Internet beschrieben:

1. Die Diensteanbieter sollten jeden Benutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationales Datenschutzrecht geregelt. Dies bedeutet z. B. daß personenbezogene Daten nur auf eine nachvollziehbare Art und Weise gespeichert werden dürfen. Medizinische und andere besonders sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den an das Internet angeschlossenen Computern gespeichert werden. Polizeiliche Steckbriefe und Fahndungsaufrufe sollten nicht im Internet veröffentlicht werden.

3. Initiativen für eine engere internationale Zusammenarbeit, ja sogar für eine internationale Konvention, die den Datenschutz im Zusammenhang mit grenzüberschreitenden Computernetzen und Diensten regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen.

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwickelt werden. Insbesondere die Nutzung sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von „Qualitätsstempeln“ für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten „Netiquette“ und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

Bericht

Das Internet ist gegenwärtig das größte internationale Computernetz der Welt. In mehr als 140 Ländern gibt es „Auffahrten“ zu dieser „Datenautobahn“. Das Internet besteht aus mehr als vier Millionen angeschlossenen Rechnern („hosts“); mehr als 40 Millionen Benutzer aus aller Welt können wenigstens einen der verschiedenen Internet-Dienste nutzen und haben die Möglichkeit, miteinander durch elektronische Post zu kommunizieren. Die Benutzer haben Zugriff auf einen immensen Informationsbestand, der an verschiedenen Orten in aller Welt gespeichert wird. Das Internet kann als erste Stufe der sich entwickelnden Globalen Informationsinfrastruktur (GII) bezeichnet werden. Das World Wide Web bildet als die modernste Benutzeroberfläche im Internet eine Basis für neue interaktive Multimedia-Dienste. Die Internet-Protokolle werden zunehmend auch für die Kommunikation innerhalb großer Unternehmen genutzt („Intranet“).

Die Teilnehmer am Internet haben unterschiedliche Aufgaben, Interessen und Möglichkeiten:

- Die Software-, Computer- und Telekommunikationsindustrien erstellen die Kommunikationsnetze und die angebotenen Dienste.

- Telekommunikationsorganisationen wie die nationalen Telekommunikationsunternehmen stellen die Basisnetze für die Datenübertragung zur Verfügung (Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen).

- Dienstleistungsunternehmen stellen Basisdienste für die Speicherung, Übertragung und Darstellung von Daten zur Verfügung. Sie sind für den Datentransport im Internet verantwortlich (routing, delivery) und verarbeiten Verbindungsdaten.

- Informationsanbieter stellen den Benutzern in Dateien und Datenbanken gespeicherte Informationen zur Verfügung.

- Die Benutzer greifen auf die verschiedenen Internet-Dienste (elektronische Post, news, Informationsdienste) zu und nutzen das Netz sowohl zur Unterhaltung als auch für Teleshopping, Telearbeit, Fernunterricht und Telemedizin.

I. Probleme und Risiken

Anders als bei der traditionellen Verarbeitung personenbezogener Daten, bei der normalerweise eine einzelne Behörde oder ein Unternehmen für den Schutz der personenbezogenen Daten ihrer Kunden verantwortlich ist, ist im Internet eine solche Gesamtverantwortung keiner bestimmten Einrichtung zugewiesen. Darüber hinaus gibt es keinen internationalen Kontrollmechanismus zur Erzwingung der Einhaltung gesetzlicher Verpflichtungen, soweit diese existieren. Der Benutzer muß daher Vertrauen in die Sicherheit des gesamten Netzes setzen, das bedeutet in jeden einzelnen Bestandteil des Netzes, unabhängig davon, wo dieser angesiedelt ist oder von wem er verwaltet wird. Die Vertrauenswürdigkeit des Netzes wird durch die Einführung neuer Software, bei deren Nutzung Programme aus dem Netz geladen werden und die mit einer Verschlechterung der Kontrolle der auf dem Rechner des Benutzers gespeicherten personenbezogenen Daten verbunden ist, sogar noch wichtiger werden.

Die schnelle Ausbreitung des Internet und seine zunehmende Nutzung für kommerzielle und private Zwecke führen zur Entstehung schwerwiegender Datenschutzprobleme:

- Das Internet ermöglicht die schnelle Übertragung großer Informationsmengen auf beliebige andere an das Netzwerk angeschlossene Computersysteme. Sensible personenbezogene Daten können in Länder übertragen werden, die nicht über ein angemessenes Datenschutzniveau verfügen. Informationsanbieter könnten personenbezogene Daten auf Rechnern in Ländern ohne jegliche Datenschutzgesetzgebung anbieten, auf die aus aller Welt durch einen einfachen Mausklick zugegriffen werden kann.

- Personenbezogene Daten können über Länder ohne jegliche oder ohne hinreichende Datenschutzgesetzgebung geleitet werden. Im Internet, das ursprünglich für akademische Zwecke eingerichtet wurde, ist die Vertraulichkeit der Kommunikation nicht sichergestellt.

Es gibt keine zentrale Vermittlungsstelle oder sonstige verantwortliche Einrichtung, die das gesamte Netz kontrolliert. Damit ist die Verantwortung für Datenschutz und Datensicherheit auf Millionen von Anbietern verteilt. Eine übertragene Nachricht könnte an jedem Computersystem, das sie passiert, abgehört und zurückverfolgt, verändert, gefälscht, unterdrückt oder verzögert werden. Trotzdem nimmt die Nutzung des Internet für Geschäftszwecke exponentiell zu, und personenbezogene und andere sensible Daten (Kreditkarten-Informationen und Gesundheitsdaten) werden über das Internet übertragen.

- Bei der Nutzung von Internet-Diensten wird weder eine angemessene Anonymität noch eine angemessene Authentifizierung sichergestellt. Computernetzwerk-Protokolle und viele Internet-Dienste arbeiten in der Regel mit dedizierten (Punkt-zu-Punkt-)Verbindungen. Zusätzlich zu den Inhaltsdaten wird dabei die Identität (ID) von Sender und Empfänger übertragen. Jeder elektronische Brief enthält einen „header" mit Informationen über Sender und Empfänger (Name und IP-Nummer, Name des Rechners, Zeitpunkt der Übertragung). Der „header" enthält weitere Informationen über den Übertragungsweg und den Inhalt der Nachricht. Er kann auch Hinweise auf Publikationen anderer Autoren enthalten. Die Benutzer sind gezwungen, eine elektronische Spur zu hinterlassen, die zur Erstellung eines Benutzerprofils über persönliche Interessen und Vorlieben verwendet werden kann. Obwohl es keinen zentralen Abrechnungsmechanismus für Zugriffe auf news oder das World Wide Web gibt, kann das Informationsgebaren von Sendern und Empfängern zumindest von dem Dienstleistungsunternehmen, an das der Benutzer angeschlossen ist, verfolgt und überwacht werden.

- Andererseits sind die unzureichenden Identifizierungs- und Authentifizierungsprozeduren im Internet bereits dazu benutzt worden, in unzureichend geschützte Computersysteme einzudringen, auf dort gespeicherte Informationen zuzugreifen und diese zu verändern oder zu löschen. Das Fehlen einer sicheren Authentifikation könnte auch genutzt werden, um auf kommerzielle Dienste auf Kosten eines anderen Benutzers zuzugreifen.

- Es gibt im Internet Tausende von speziellen news-groups, von denen die meisten jedem Nutzer offenstehen. Die Artikel können personenbezogene Daten von Dritten enthalten, die gleichzeitig auf vielen tausend Computersystemen gespeichert werden, ohne daß der Einzelne eine Möglichkeit hat, dagegen vorzugehen.

Die Teilnehmer am Internet haben ein gemeinsames Interesse an der Integrität und Vertraulichkeit der übertragenen Information: Die Benutzer sind an verläßlichen Diensten interessiert und erwarten, daß ihre personenbezogenen Daten geschützt werden. In bestimmten Fällen können sie ein Interesse daran haben, Dienste ohne

Identifizierung benutzen zu können. Den Benutzern ist es normalerweise nicht bewußt, daß sie beim „Surfen“ im Netz einen globalen Marktplatz betreten und daß jeder einzelne Schritt dort überwacht werden kann.

Andererseits sind viele Diensteanbieter an der Identifizierung und Authentifizierung von Benutzern interessiert: Sie benötigen personenbezogene Daten für die Abrechnung, könnten diese Daten aber auch für andere Zwecke nutzen. Je mehr das Internet für kommerzielle Zwecke genutzt wird, desto interessanter wird es für Diensteanbieter und andere Einrichtungen sein, so viele Verbindungsdaten über das Nutzerverhalten im Netz wie möglich zu speichern und damit das Risiko für den Datenschutz der Kunden zu verstärken. Unternehmen bieten in zunehmendem Maße freien Zugang zum Internet an, um sicherzustellen, daß die Kunden ihre Werbeanzeigen lesen, die zu einer der hauptsächlichen Finanzierungsquellen des gesamten Internets werden. Die Unternehmen wollen nachvollziehen können, in welchem Ausmaß, von wem und wie oft ihre Werbeanzeigen gelesen werden.

Im Hinblick auf die erwähnten Risiken kommt den Einrichtungen, die das Netz auf internationaler, regionaler und nationaler Ebene verwalten, insbesondere bei der Entwicklung der Protokolle und Standards für das Internet, bei der Festlegung der Regeln für die Identifikation der angeschlossenen Server und schließlich bei der Identifikation der Benutzer eine wichtige Funktion zu.

II. Vorhandene Regelungen und Empfehlungen

Obwohl verschiedene nationale Regierungen und internationale Organisationen (z. B. die Europäische Union) Programme gestartet haben, um die Entwicklung von Computernetzen und -diensten zu erleichtern und zu intensivieren, sind dabei nur sehr geringe Anstrengungen unternommen worden, um für ausreichende Datenschutz- und Datensicherheitsregelungen zu sorgen. Einige nationale Datenschutzbehörden haben bereits Empfehlungen für die technische Sicherheit von an das Internet angeschlossenen Computernetzen und über Datenschutzrisiken für die einzelnen Benutzer von Internet-Diensten herausgegeben. Solche Empfehlungen sind z. B. in Frankreich, Großbritannien (vgl. den 11. Jahresbericht des Data Protection Registrar, Anhang 6) und in Deutschland erarbeitet worden. Die wesentlichen Punkte können wie folgt zusammengefaßt werden:

- Das Anbieten von Informationen auf dem Internet fällt in den Regelungsbereich der nationalen Datenschutzgesetze und -regelungen. In dieser Hinsicht ist das Internet nicht so ungeregelt, wie oft behauptet wird. Es ist, um nur ein Beispiel zu nennen, einem deutschen Anbieter eines WorldWideWebServers verboten, ohne Wissen des Benutzers die vollständigen Angaben über den auf ihr Angebot zugreifenden Rechner, die abgerufenen Seiten und heruntergela-

dene Dateien zu speichern (wie es im Netz allgemein praktiziert wird). Nationale Regelungen können eine Verpflichtung für Informationsanbieter enthalten, sich bei einer nationalen Datenschutzbehörde anzumelden. Nationale Gesetze enthalten darüber hinaus spezielle Regelungen im Hinblick auf internationales Straf-, Privat- und Verwaltungsrecht (Kollisionsrecht), die unter bestimmten Umständen Lösungen bereitstellen können.

- Bevor ein lokales Computernetz – z. B. das einer Behörde – an das Internet angeschlossen wird, müssen die Risiken für das lokale Netzwerk und die darauf gespeicherten Daten im Einklang mit dem nationalen Recht abgeschätzt werden. Dazu kann die Erarbeitung eines Sicherheitskonzepts und einer Abschätzung, ob es erforderlich ist, das gesamte Netz oder nur Teile davon an das Internet anzuschließen, gehören. Abhängig von dem verfolgten Zweck kann es sogar ausreichend sein, nur ein Einzelplatzsystem an das Netz anzuschließen. Es sollten technische Maßnahmen getroffen werden, um sicherzustellen, daß auf dem Internet nur auf Daten, die veröffentlicht werden könnten, zugegriffen werden kann, z. B. durch Einrichtung eines Firewall-Systems, das das lokale Netzwerk vom Internet trennt. Es muß jedoch festgestellt werden, daß der Anschluß eines Computernetzwerks an das Internet eine Erhöhung des Sicherheitsrisikos auch dann bedeutet, wenn solche technischen Maßnahmen getroffen worden sind.

- Falls personenbezogene Daten von Nutzern eines bestimmten Dienstes gespeichert werden, muß für die Benutzer klar sein, wer diese Daten nutzen wird und zu welchen Zwecken die Daten genutzt oder übermittelt werden sollen. Dies bedeutet eine Information am Bildschirm vor der Übermittlung und die Schaffung einer Möglichkeit, die Übermittlung zu unterbinden. Der Benutzer sollte in der Lage sein, diese Unterrichtung und aller übrigen Bedingungen, die durch den Diensteanbieter gestellt werden, auszudrucken.

- Wenn der Zugang zu personenbezogenen Daten auf einem Computersystem bereitgestellt wird – z. B. durch die Veröffentlichung biographischer Angaben über Mitarbeiter in einem Verzeichnis – muß der Informationsanbieter sicherstellen, daß diese Personen sich der globalen Natur des Zugriffs bewußt sind. Am sichersten ist es, die Daten nur mit der informierten Einwilligung der betroffenen Person zu veröffentlichen.

Darüber hinaus gibt es eine Reihe von internationalen gesetzlichen Bestimmungen und Konventionen, die u. a. auch auf das Internet anwendbar sind:

- Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, verabschiedet vom Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) am 23. September 1980

- Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981

- Richtlinien betreffend personenbezogene Daten in automatisierten Dateien, von der Generalversammlung der Vereinten Nationen verabschiedet am 4. Dezember 1990

- Richtlinie des Rates der Europäischen Gemeinschaften 90/387/EWG vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision – ONP) (in der Datenschutz als „grundlegende Anforderung" definiert wird)

- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie)

- Allgemeines Abkommen über Handel und Dienstleistungen (GATS) (das in Artikel XIV regelt, daß die Mitgliedstaaten durch das weltweite Abkommen nicht daran gehindert werden, Regelungen über den Datenschutz von Einzelpersonen im Zusammenhang mit der Verarbeitung und Verbreitung von personenbezogenen Daten und dem Schutz der Vertraulichkeit von Akten und Aufzeichnungen über Einzelpersonen zu erlassen oder durchzusetzen).

Die Richtlinie der Europäischen Union enthält als erstes supra-nationales Gesetzeswerk eine wichtige Neudefinition des Begriffs „für die Verarbeitung Verantwortlicher", die im Zusammenhang mit dem Internet von Bedeutung ist. Artikel 2 Buchstabe c) definiert den „für die Verarbeitung Verantwortlichen" als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Wenn man diese Definition auf die Nutzung des Internet für die Zwecke der Übermittlung elektronischer Post anwendet, muß der Absender einer elektronischen Nachricht als „für die Verarbeitung Verantwortlicher" dieser Nachricht angesehen werden, wenn er eine Datei mit personenbezogenen Daten absendet, da er die Zwecke und Mittel der Verarbeitung und Übermittlung dieser Daten bestimmt. Andererseits bestimmt der Anbieter eines Mailbox-Dienstes selbst die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Betrieb des Mailbox-Dienstes und hat damit wenigstens eine Mitverantwortung für die Einhaltung der anwendbaren Regelungen über den Datenschutz.

Kürzlich hat die Europäische Kommission zwei Dokumente veröffentlicht, die zu einer europäischen Gesetzgebung führen könnten und in diesem Fall beträchtliche Auswirkungen auf den Datenschutz im Internet haben werden:

Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über illegale und schädigende Inhalte im Internet (KOM(96) 487)

und

Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und Informationsdiensten (KOM(96) 483).

Obwohl auch diese nicht rechtlich bindend und eher auf einer nationalen denn auf einer internationalen Ebene verabschiedet worden sind, sollten die

- Grundsätze für die Bereitstellung und Nutzung personenbezogener Daten
  „Privacy und die nationale Informations-Infrastruktur"
  verabschiedet von der Privacy Working Group
  des Information Policy Committee
  innerhalb der Information Infrastructure Task Force (IITF) am 6. Juni 1995

genannt werden, da sie einen Einfluß auf die internationalen Datenflüsse haben werden. Sie sind intensiv und fruchtbar mit der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation bei einem gemeinsamen Treffen in Washington D. C. am 28. April 1995 diskutiert worden.

In der Praxis werden einige wichtige und effektive Regeln zur Selbstregulierung von der Netzgemeinde selbst aufgestellt (z. B. „Netiquette"). Solche Maßnahmen dürfen im Hinblick auf die Rolle, die sie gegenwärtig und zukünftig für den Datenschutz des einzelnen Benutzers spielen können, nicht unterschätzt werden. Sie tragen mindestens dazu bei, die nötige Aufmerksamkeit unter den Benutzern dafür zu schaffen, daß Vertraulichkeit als eine Grundanforderung auf dem Netz nicht existiert („Sende oder speichere niemals etwas in Deiner Mailbox, das Du nicht in den Abendnachrichten sehen möchtest"). Die EU-Datenschutzrichtlinie wiederum fordert Verhaltensregeln (Artikel 27), die von den Mitgliedstaaten und der Kommission gefördert werden sollen.

III. Empfehlungen

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz im Internet im Augenblick unzureichend ist.

Das Recht jedes Einzelnen, die Datenautobahn zu benutzen, ohne überwacht und identifiziert zu werden, sollte garantiert werden. Andererseits muß es im Hinblick auf die Nutzung personenbezogener Daten auf der Datenautobahn (z. B. von Dritten) Grenzen geben („Leitplanken").

Eine Lösung für dieses Grunddilemma muß auf folgenden Ebenen gefunden werden:

1. Die Diensteanbieter sollten jeden potentiellen Nutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. Da „sowohl die einzelnen Teile der Netzwerk-Infrastruktur als auch die Benutzer jeder einen physikalischen Standort haben, können Staaten einen bestimmten Grad von Verläßlichkeit in bezug auf die Netze und ihre Teilnehmer verhängen und durchsetzen“ (Joel Reidenberg). In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationale Datenschutzgesetze geregelt.

   Personenbezogene Daten dürfen nur in einer nachvollziehbaren Art und Weise gespeichert werden. Medizinische und andere sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den am Internet angeschlossenen Computern gespeichert werden.

   Es spricht viel dafür, die Nutzung des Internet für die Veröffentlichung von Steckbriefen und Fahndungsaufrufen durch die Polizei zu verbieten (das amerikanische Federal Bureau of Investigations veröffentlicht seit einiger Zeit eine Liste von gesuchten Verdächtigen im Internet). Die beschriebenen Defizite der Authentifizierungsprozeduren und die leichte Manipulierbarkeit von Bildern im Cyberspace scheinen die Nutzung des Internet für diesen Zweck auszuschließen.

3. Verschiedene nationale Regierungen haben internationale Übereinkommen über die globale Informations-Infrastruktur angeregt. Initiativen für eine engere internationale Zusammenarbeit, ja sogar eine internationale Konvention, die den Datenschutz im Hinblick auf grenzüberschreitende Netze und Dienste regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen. Konzepte für solche Maßnahmen sind bereits entwickelt und veröffentlicht worden. Beispiele sind das „Identity-Protector"-Konzept, das in „Privacy-enhancing technologies: The path to anonymity" von der niederländischen Registratiekamer und dem Datenschutzbeauftragten von Ontario/Kanada enthalten ist (vorgestellt auf der 17. Internationalen Konferenz der Datenschutzbeauftragten in Kopenhagen (1995)) und das „User Agent-Konzept", das auf der gemeinsamen Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation und der Privacy Working Group der Information Infrastructure Task Force vorgestellt wurde (April 1995).

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwickelt werden.

   Die Nutzung sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

   Die Arbeitsgruppe unterstützt neue Entwicklungen im Internet-Protokoll (z. B. IP v6), die die Vertraulichkeit durch Verschlüsselung, Klassifizierung von Nachrichten und bessere Authentifizierungsprozeduren verbessern. Die Hersteller von Software sollten den Sicherheitsstandard des neuen Internet-Protokolls in ihre Produkte aufnehmen und Diensteanbieter sollten die Nutzung dieser Produkte so schnell wie möglich unterstützen.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von „Qualitätsstempeln" für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten „Netiquette" und datenschutzfreundliche Techno-

logie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die weitere Entwicklung in diesem Bereich genau beobachten, Anregungen aus der Netzgemeinde berücksichtigen und weitere, detailliertere Vorschläge entwickeln.

20th meeting, 18th and 19th November 1996, Berlin

Report and Guidance on Data Protection and Privacy on the Internet ("Budapest – Berlin Memorandum")

Summary

There can be no doubt that the legal and technical protection of Internet users' privacy is at present insufficient**.**

Ten guiding principles are set out in this document to improve privacy protection on the Net:

1. Service providers should inform each user of the Net unequivocally about the risks to his privacy. He will then have to balance these risks against the expected benefits.

2. In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law. This means e.g. that personal data may only be collected in a transparent way. Patients' data and other sensitive personal data should only be communicated via the Internet or be stored on computers linked to the Net if they are encrypted. Arrest warrants issued by the police should not be published on the Internet.

3. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of transborder networks and services are to be supported.

4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies.

Responsibility for privacy protection will have to be institutionalized to a certain extent.

5. National and international law should state unequivocally that the process of communicating (e.g. via electronic mail) is also protected by the secrecy of telecommunications and correspondence.

6. Furthermore it is necessary to develop technical means to improve the user's privacy on the Net. It is mandatory to develop design principles for information and communications technology and multimedia hard- and software which will enable the individual user to control and give him feedback with regard to his personal data. In general users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.

7. Technical means should also be used for the purpose of protecting confidentiality. In particular the use of secure encryption methods must become and remain a legitimate option for any user of the Internet.

8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification issuing "quality stamps" for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.

9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.

10. Finally it will be decisive to find out how self-regulation by way of an expanded "Netiquette" and privacy-friendly technology might improve the implementation of national and international regulations on privacy protection**.** It will not suffice to rely on any one of these courses of action: they will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.

Report

Today, the Internet is the world's largest international computer network. There are "slip roads" to this "Information Superhighway" in more than 140 countries. The Internet consists of more than four millions of Internet sites ("hosts"); more than 40 millions of users from all over the world can use at least one of the different Internet services and have the facilities to communicate with each other via electronic mail. Users have access to an immense pool of information stored at

different locations all over the world. The Internet can be regarded as the first level of the emerging Global Information Infrastructure (GII).The WorldWideWeb as the most modern Internet user interface is a basis for new interactive multimedia services. Internet protocols are increasingly being used for communications within large companies ("Intranets").

The participants in the Internet have different tasks, interests and opportunities:

- The software, computer and telecommunications industries design the networks and the services available.

- Telecommunications organisations like national telecoms provide basic networks for data transfer (point-to-point or point-to-multipoint connections).

- Access (communications) providers supply basic services for storage, transmission and presentation. They are responsible for the Internet transport system (routing, delivery) and process traffic data.

- Information (content) providers supply information stored in files and databases to the users.

- Users access different kinds of Internet services (mail, news, information) and use the Net for entertainment as well as for teleshopping, teleworking, teleteaching/ -learning and telemedecine.

I. Problems and risks

Unlike in traditional processing of personal data where there is usually a single authority or enterprise responsible for protecting the privacy of their customers, there is no such overall responsibility on the Internet assigned to a certain entity. Furthermore there is no international oversight mechanism to enforce legal obligations as far as they exist. Therefore the user is forced to put trust into the security of the entire network, that is every single component of the network, no matter where located or managed by whom. The trustworthiness of the Net will become even more crucial with the advent of new software which induces the user not only to download programs from the Net, but also weakens his control over his personal data.

The fast growth of the Internet and its increasing use for commercial and private purposes give rise to serious privacy problems:

- The Internet facilitates the quick transmission of great quantities of information to any computer system connected to the network. Sensitive personal data can be communicated to countries without an appropriate data protection level.

Information providers might offer personal data from sites situated in countries without any privacy legislation where they can be accessed from all over the world by a simple mouse click.

- Personal data may be routed via countries without any or without sufficient data protection legislation. On the Internet, basically built for academic purposes, confidential communication is not ensured.

  There is no central switching center or other responsible authority in control of the entire network. Therefore the responsibility for data protection and data security is shared between millions of providers. Every message transmitted could be intercepted at any site it passes and could be traced, changed, forged, suppressed or delayed. Nevertheless the Internet use for business purposes increases exponentially and personal and other sensitive data (credit card data as well as individual health information) are transmitted via the Internet.

- The use of Internet services does not allow for adequate anonymity nor adequate authentification. Computer network protocols and many Internet services generally work with dedicated (point-to-point-) connections. In addition to the content data the identification (ID) of the sender and the recipient is transmitted. Every electronic mail message contains a header with information about the sender and the recipient (name and IP-address, host name, time of the mailing). The header contains further information on the routing and the subject of the message. It may also contain references to articles by other authors. Users are bound to leave an electronic trace which can be used to develop a profile of personal interests and tastes. Although there is no central accounting of the access to news or WorldWideWeb, the information behaviour of senders and recipients can be traced and supervised at least by the communications provider to whom the user is connected.

- On the other hand, the weakness of identification and authentication procedures on the Internet has been used to penetrate remote computer systems which were insufficiently protected, to spy on the information stored and to manipulate or delete it. The lack of secure authentication could also be used to access commercial services at the cost of another user.

- There are thousands of special news-groups in the Internet; most of them are open for every user. The contents of articles may contain personal data of third persons; this personal information is simultaneously stored on many thousands of computer systems without any right of redress for the individual.

The participants in the Internet share an interest in the integrity and confidentiality of the information transmitted: Users are interested in reliable services and expect their privacy to be protected. In some cases they may be interested in us-

ing services without being identified. Users do not normally realize that they are entering a global market-place while surfing on the Net and that every single movement may be monitored.

On the other hand many providers are interested in the identification and authentication of users: They want personal data for charging, but they could also use these data for other purposes. The more the Internet is used for commercial purposes, the more interesting it will be for service providers and other bodies to get as much transaction-generated information about the customer's behaviour on the Net as possible, thus increasing the risk to the customer's privacy. Increasingly companies start to offer free access to the Net as a way of assuring that customers read their advertisements which become a major financing method for the whole Internet. Therefore they want to follow to want extent, by whom and how often their advertisements are being read.

With regard to certain risks mentioned the functions of the bodies which on an international, regional and national level manage the Net are important in particular when they develop the protocols and standards for the Internet, fix rules for the identification of servers connected and eventually for the identification of users.

II. Existing regulations and guidelines

Although several national governments and international organisations (for example the European Union) have launched programmes to faciliate and intensify the development of computer networks and services, only very little efforts have been taken to provide for sufficient data protection and privacy regulations in this respect. Some national Data Protection Authorities have already issued guidelines on the technical security of computer networks linked to the Internet and on privacy risks for the individual user of Internet services. Such guidelines have been laid down for example in France, in the U.K. (see the 11th Annual Report of the Data Protection Registrar, Appendix 6) and in Germany. The main topics can be summed up as follows:

Providing information on the Internet is subject to the national data protection laws and regulations. In this respect the Internet is not as unregulated as often stated. It is, to name but one example, illegal for a German provider of a WorldWideWebServer to register the complete addresses of computers which have accessed which Web pages and to which files are being downloaded without the knowledge of the person initiating that procedure (as is the usual practice on the Net). National regulations might include the obligation for information providers to register at a national data protection authority. National law also contains specific provisions with regard to international criminal, private and administrative law (conflict of laws) which may provide solutions in certain circumstances.

- Before connecting a local computer network – for example of a public authority – to the Internet the risks for the security of the local network and the data stored there have to be assessed in conformity with the national law. This may include drawing up a security plan and assessing whether it is necessary to connect the entire network or only parts of it to the Internet. Depending on the purpose it might even be sufficient to connect only a stand-alone system to the Net. Technical measures should be taken to secure that only the data which could be published can be accessed on the Internet for example by setting up a firewall system separating the local network from the Net. However, it should be noted that even if such technical steps have been taken connecting a computer network to the Internet means putting an additional risk to its security.

- If personal data on users of a service are collected it must be clear to them who is to use the data and what are the purposes for which the data are to be used or disclosed. This means giving notification on the screen before disclosure and providing an opportunity to prevent disclosure. The user should be able to make a hardcopy of this notification and of any other terms and conditions set by the provider.

- If access to personal data on a computer system is provided – for example by publishing biographical details of staff members in a directory – the information provider must make sure that those individuals understand the global nature of that access. The safe course is to publish the data only with the informed consent of the persons concerned.

There are also a number of international legal regulations and conventions that apply inter alia to the Internet:

– Recommendation with Guidelines on the protection of privacy and transborder flows of personal data adopted by the Council of the Organisation for Economic Cooperation and Development (OECD) on 23 September 1980

– Council of Europe Convention No. 108 for the protection of individuals with regard to automatic processing of personal data adopted on 28 January 1981

– Guidelines for the regulation of computerized personal data files adopted by the United Nations General Assembly on 14 December 1990

– European Council 90/387/EEC of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of Open Network Provision (ONP) and ensuing ONP Directives (defining data protection as “essential requirement”)

– Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU-Data Protection-Directive)

– General Agreement on Trade and Services (GATS) (stating in Article XIV that Member States are not prevented by this worldwide agreement to adopt or enforce regulations relating to the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.

The EU-Directive as the first supra-national legal instrument does contain an important new definition of "controller" which is relevant in the Internet context. Article 2 lit. c) defines "controller" as the natural and legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Applying this definition to the use of the Internet for purposes of electronic mail the sender of an electronic message has to be considered to be the controller of this message when sending a file of personal data for he determines the purposes and means of the processing and transmission of those personal data. On the other hand the provider of a mailbox service himself determines the purposes and means of the processing of the personal data related to the operation of the mailbox service and therefore he as "controller" has at least a joint responsibility to follow the applicable rules of data protection.

More recently the European Commission has published two documents which might lead to Union legislation and will in that event have considerable consequences on data protection on the Internet:

Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the Internet (COM(96) 487)

and

Green Paper on the protection of minors and human dignity in audiovisual and information services (COM(96) 483).

Although not legally binding either and adopted on a national rather than an international level the

- Principles for providing and using personal information
  "Privacy and the National Information Infrastructure"
  adopted by the Privacy Working Group

of the Information Policy Committee
within the United States Information Infrastructure Task Force (IITF) on 6 June 1995

should be mentioned in this context for they are bound to influence the international data flows. They have been discussed intensively and fruitfully with the International Working Group on Data Protection in Telecommunications at the Joint Meeting in Washington, D.C., on 28 April 1995.

In practice some important and effective rules are being imposed by the Net Community themselves by way of self-regulation (e.g. "Netiquette"). Such methods are not to be under-estimated as to the role they play and might play in future in protecting the individual user's privacy. At least they contribute to creating the necessary awareness among users that confidentiality on the Net as a basic standard is non-existent ("Never send or keep anything in your mailbox that you would mind seeing on the evening news.") The EU-Data Protection Directive in turn calls for codes of conduct (Article 27) which should be encouraged by Member States and the Commission**.**

III. Guidance

There can be no doubt that the legal and technical protection of Internet users' privacy is at present insufficient**.**

On the one hand the right of every individual to use the Information Superhighway without being observed and identified should be guaranteed. On the other hand there have to be limits (crash-barriers) with regard to the use of personal data (e.g. of third persons) on the highway.

A solution to this basic dilemma will have to be found on the following levels:

1. Service providers should inform each potential user of the Net unequivocally about the risks to his privacy. He will then have to balance these risks against the expected benefits.

2. As "elements of network infrastructure as well as participants each have physical locations, states have the ability to impose and enforce a certain degree of liability on networks and their participants**"** (Joel Reidenberg). In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law.

   Personal data may only be collected in a transparent way. Patients' data and other sensitive personal data should only be communicated via the Internet or be stored on computers linked to the Net if they are encrypted**.**

There is also a strong case to prohibit the use of the Internet for the publication of arrest warrants by the police (the U.S. Federal Bureau of Investigations has published a list of wanted suspects on the Net for some time and other national police authorities are following this example). The described deficiencies in the authentication procedure and the easy manipulation of pictures in Cyberspace seem to prevent the use of the Net for this purpose.

3. Several national governments are calling for international agreements on the Global Information Infrastructure. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of transborder networks and services are to be supported.

4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies. Responsibility for privacy protection will have to be institutionalized to a certain extent.

5. National and international law should state unequivocally that the process of communicating (e.g. via electronic mail) is also protected by the secrecy of telecommunications and correspondence.

6. Furthermore it is necessary to develop technical means to improve the user's privacy on the Net. It is mandatory to develop design principles for information and communications technology and multimedia hard- and software which will enable the individual user to control and give him feedback with regard to his personal data. In general users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service. Concepts for such measures have already been developed and published. Examples are the "Identity Protector" concept included in "Privacy-enhancing technologies: The path to anonymity" by the Dutch Registratiekamer and The Information and Privacy Commissioner of Ontario/Canada (presented at the 17th International Conference on Data Protection in Copenhagen (1995) and the "User Agent-concept" as reported on at the joint Washington meeting of the Working Group with the Privacy Working Group of the IITF (April 1995).

7. Technical means should also be used for the purpose of protecting confidentiality.

   The use of secure encryption methods must become and remain a legitimate option for any user of the Internet.

   The Working Group supports new developments of the Internet Protocol (e.g. IP v6) which offer means to improve confidentiality by encryption, clas-

sification of messages and better authentication procedures. The software manufacturers should implement the new Internet Protocol security standard in their products and providers should support the use of these products as quickly as possible.

8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification issuing "quality stamps" for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.

9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.

10. Finally it will be decisive to find out how self-regulation by way of an expanded "Netiquette" and privacy-friendly technology might improve the implementation of national and international regulations on privacy protection**.** It will not suffice to rely on any one of these courses of action: they will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.

The International Working Group on Data Protection in Telecommunications will monitor the developments in this field closely, take into account comments from the Net Community and develop further more detailed proposals.

Bericht und Empfehlungen zu Telekommunikation und Datenschutz im Arbeitsverhältnis (August 1996)

Vorbemerkung

Das Ziel dieses Berichtes ist es, eine Reihe von Empfehlungen zum Einsatz von Informations- und Telekommunikationstechnik zu geben, soweit sie zur Erhebung vom Arbeitnehmerdaten benutzt werden.

Ihr Einsatz hat die Methoden zur Erhebung und Verarbeitung von Daten am Arbeitsplatz drastisch verändert und vervielfacht. Ständige Überwachung und Erhebung von Daten über verschiedene Aspekte des Verhaltens der Arbeitnehmer – evtl. ohne ihr Wissen – ist möglich. Diese neuen Methoden werden zunehmend verfügbar, und sie werden allmählich am Arbeitsplatz akzeptiert. Ihr Einsatz erfolgt aus Gründen der Sicherheit, der Kontrolle und Zuordnung von Kosten verschiedener Leistungen und Kommunikationsvorgänge sowie zur Mes-

sung und Verbesserung der Produktivität. Zugleich bieten sie aber ein großes Potential der Sammlung und Verarbeitung der Daten über das persönliche Verhalten, die Aktivitäten und Persönlichkeitsmerkmale des Arbeitnehmers. Die Gefahr von Verletzungen der Privat-sphäre des Arbeitnehmers ist erheblich und muß deshalb aus der Sicht des Datenschutzes berücksichtigt werden.

Der Begriff des „Arbeitsplatzes" ist in diesem Zusammenhang weit zu verstehen, als jeder Ort, an dem der Arbeitnehmer sich aufhält, wenn er Tätigkeiten auf Anweisung seines Arbeitgebers ausübt. Dies können sowohl der Arbeitsplatz im Unternehmen als auch das Fahrzeug des Arbeitnehmers oder dessen Privatwohnung sein. In dieser Hinsicht erfordern die neueren Entwicklungen im Bereich der Telearbeit besondere Aufmerksamkeit.

Der erste Teil des Berichts gibt einen Überblick über die Methoden der Datenerhebung auf der Grundlage der Informations- und Telekommunikationstechnik, die am Arbeitsplatz eingesetzt werden, und ihr Potential zur Erhebung von arbeitnehmerbezogenen Informationen.

In einem zweiten Teil wird eine Reihe von Empfehlungen zum Schutz der Privatsphäre am Arbeitsplatz gegeben. In erster Linie werden einige verfahrensmäßige Bedingungen formuliert, die beachtet werden sollten, wenn Vorrichtungen zur Sammlung von Daten am Arbeitsplatz eingesetzt werden. Zum zweiten wird das Recht des Arbeitnehmers auf Schutz seiner Privatsphäre materiell beschrieben.

Im dritten und letzten Teil werden drei spezielle Anwendungen dieser Empfehlungen auf Informations- und Telekommunikationstechnologie beschrieben.

In diesem Zusammenhang ist zu erwähnen, daß die Empfehlung Nr. R (89)2 zum Schutz personenbezogener Daten im Arbeitsverhältnis vom Ministerkomitee des Europarats am 18. Januar 1989 bei der 324. Sitzung der stellvertretenden Minister angenommen worden ist. Die Prinzipien dieser Empfehlung gelten insbesondere für die Erhebung und Nutzung personenbezogener Daten für arbeitsrechtliche Zwecke im öffentlichen und privaten Bereich.

Außerdem hat die Internationale Arbeitsorganisation 1995 den Entwurf eines Verhaltenskodex zum Arbeitnehmerdatenschutz veröffentlicht.

Schließlich wird die Frage des Arbeitnehmerdatenschutzes gegenwärtig von der Generaldirektion V der Europäischen Kommission untersucht.

Die Empfehlungen, die im folgenden gegeben werden, konzentrieren sich insbesondere auf den Einsatz und die Nutzung von Telekommunikations- und Informationstechnik zur Erhebung und Verarbeitung von arbeitnehmerbezogenen Daten. Ihre schnell wachsende Akzeptanz am Arbeitsplatz, ihr erhebliches Poten-

tial zur Erhebung und Verarbeitung personenbezogener Daten für verschiedene Zwecke machen es notwendig, sie unter dem Gesichtspunkt des Datenschutzes zu überprüfen. Angesichts des gegenwärtigen Mangels an Regulierung in diesem Bereich könnten eine Reihe von Empfehlungen ein nützliches Werkzeug für Arbeitgeber sein, die bereit sind, die Regeln zum Arbeitnehmerdatenschutz zu beachten.

I. Auf Informations- und Telekommunikationstechnologie basierende Methoden der Datenerhebung und -verarbeitung

1. Basierend auf der Nutzung von Computern, Telekommunikations- oder audiovisuellen Technologien findet ein breites Spektrum von Geräten zur Aufzeichnung von Daten am Arbeitsplatz zunehmende Akzeptanz:

   – „active badges" (Badge-Systeme) (auch „Tabs" oder neutraler „Netzwerk Standortgeräte" genannt) sind nur wenige Zentimeter groß und werden z. B. von den Firmen Olivetti und Bellcore angeboten. Sie enthalten einen Mikroprozessor und Infrarotsendeeinrichtungen, die die Identität ihrer Träger aussenden und alle Arten von Aktivitäten anderer informationstechnischer Geräte auslösen können, wie z. B. automatische Anrufweiterleitung, Autorisierung des Zugangs zu Gebäuden und Tagungsräumen und verschiedene weitere zweckmäßige Funktionen. In den falschen Händen können diese Systeme für ihren Träger zu großen Schwierigkeiten führen, insbesondere, wenn sie mit einem zentralen Computersystem verbunden sind, das Daten über die Ankunft und den Weggang der Arbeitnehmer speichert. Innerhalb von Gebäuden können die Bewegungen der Arbeitnehmer (zu Büchereien, Aufenthaltsräumen, verschiedenen Computerarbeitsplätzen etc.) und die Zeit, die sie in jedem Bereich eines Gebäudes verbracht haben, aufgezeichnet werden; Badge-Systeme, die auf der Erkennung biometrischer Identifizierungsmerkmale (wie z. B. Fingerabdrücke) basieren, bergen Risiken für die Privatsphäre, wenn diese Identifikationsmerkmale erhoben und gespeichert werden.

   – Die von den Arbeitnehmern genutzten, rechnergestützten Systeme erzeugen durch Aufzeichnung der Zeit, die zur Erfüllung einer Aufgabe gebraucht wird, oder der Anzahl von Aufgaben, die innerhalb einer bestimmten Zeitspanne erledigt werden (z. B. durch Zählung von Tastaturanschlägen, Anzahl von Fehlern, Pausenzeichen etc.), Information über den Arbeitsrhythmus. Neben der Überwachung der Nutzung können Computersysteme dazu verwendet werden, aus der Ferne auf die Personaldaten und elektronische Nachrichten der Arbeitnehmer zuzugreifen als auch zur Fernüberwachung des Verhaltens der Arbeitnehmer. Programme für das Projektmanagement oder die Work-Flow-Automation, die zur Steigerung der Produktivität ent-

wickelt worden sind, können die Privatsphäre der Nutzer wegen ihres Überwachungspotentials beeinträchtigen.

– Videokameras, die aus Sicherheitsgründen an Eingängen oder Orten, die ein hohes Maß an Sicherheit verlangen, plaziert werden, zeichnen personenbezogene Daten über die Arbeitnehmer auf, wie Arbeitsgewohnheiten, Verhalten, Kontakte mit Kollegen sowie auch von allen anderen betriebsfremden Personen.

– Systeme zur Abrechnung von Telefonkosten zeichnen Zeitpunkt und Dauer eingehender und ausgehender, interner und externer Gespräche auf; zusätzlich kann durch Telefonüberwachung sowohl die Anzahl anrufender oder angerufener Dritter als auch der Inhalt von dienstlichen und privaten Unterhaltungen aufgezeichnet werden; im Hinblick auf andere Telekommunikationsdienste, wie z. B. elektronische Post, können ebenfalls Maßnahmen ergriffen werden, die zur Aufzeichnung von Daten über das interne oder externe Kommunikationsverhalten der Arbeitnehmer führen.

– Die Einführung von Computern und die Ausdehnung von netzwerk- oder satellitenbasierten Kommunikationseinrichtungen in die Wohnungen, in Fahrzeugen erlauben eine Kontrolle der Arbeitnehmer von ferne, weit außerhalb der Einrichtungen des Arbeitgebers.

– Telearbeit ist ein Katalysator für die Computerisierung der Privatwohnungen der Arbeitnehmer und für die Ausbreitung von netzwerk- oder satellitengestützten Kommunikationseinrichtungen in diese Privatwohnungen. Sie werden eingerichtet, um ein Arbeitsumfeld außerhalb der Einrichtungen des Arbeitgebers zu schaffen und um die Kommunikation unter den Arbeitnehmern zu erleichtern. Satellitentechnologie für die Mobiltelefonie erlaubt die Verfolgung des Aufenthaltsorts des Arbeitnehmers außerhalb der Firma.

2. Das Eindringen in die Privatsphäre setzt entsprechende technische Möglichkeiten und eine entsprechende Haltung der Beteiligten voraus. Die folgende Aufzählung zeigt einige der Kontrollmöglichkeiten auf, die durch Informationstechnologie und Telekommunikation eröffnet werden, und ihren invasiven Charakter im Hinblick auf die Privatsphäre der Arbeitnehmer.

– Die neuen Technologien ermöglichen die Schaffung immer weiterer und genauerer Informationsquellen über die Arbeitnehmer. Ihnen wohnt ein beispielloses Potential für die Sammlung, die Messung und die Auswertung eines breiten Spektrums an Informationen nicht nur über die Leistungsfähigkeit der Arbeitnehmer, sondern auch über seine persönlichen Charakteristiken, sein Verhalten, seine Beziehung mit Kollegen und sogar mit Dritten von außerhalb des Arbeitsplatzes inne.

– Die neuen Informationstechnologien ermöglichen die kontinuierliche Kontrolle und Beobachtung am Arbeitsplatz. In bestimmten Fällen können Informationen über die Leistungsfähigkeit der Arbeitnehmer oder ihr persönliches Verhalten im geheimen gesammelt und genutzt oder für Zwecke genutzt werden, die den Arbeitnehmern nicht bewußt sind.

– In der Entwicklung hin zur Telearbeit besteht möglicherweise das wichtigste Risiko des Eindringens in die Privatsphäre von Arbeitnehmern. Die physische Entfernung zwischen dem Arbeitgeber und den Arbeitnehmern sowie zwischen den Arbeitnehmern selbst wird ein Katalysator für die Einführung von Einrichtungen zur Datenaufzeichnung werden, die eine Fernkontrolle durch den Arbeitgeber ermöglichen. Schon in dieser Entwicklung besteht ein Risiko für die Privatsphäre. Darüber hinaus könnte, da sich die Grenzen zwischen Arbeits- und Privatleben verwischen, jede unverhältnismäßige Nutzung von Aufzeichnungseinrichtungen in einem Telearbeitskontext zur Verarbeitung von sehr verschiedenen Typen von personenbezogenen Daten führen, die keine direkte Verbindung oder überhaupt keine Verbindung mit dem Arbeitsverhältnis haben.

– Eine neue Technologie, die ein Potential zur Verletzung der Privatsphäre in sich trägt, ist die Entwicklung von „medialen“ (virtuellen) Räumen (media spaces). Ein medialer Raum ist ein computergestütztes Netzwerk aus audiovisuellen Einrichtungen, das zur Unterstützung der Kommunikation und der Zusammenarbeit zwischen Personen genutzt wird, die durch die räumlichen Gegebenheiten in einem Gebäude oder geographische Distanz voneinander getrennt sind.

Jeder Raum verfügt über verschiedene Audio- und Videokabel, die mit einer Vermittlungszentrale verbunden sind und über einen Zugang zu digitalen Netzwerken verfügen. Das daraus resultierende System versorgt alle Räume mit einer Art von Audio-/Video“knoten“, bestehend aus einer Kamera, einem Monitor, einem Mikrofon und Lautsprechern. Die Verbindungen zwischen den Knoten sind vollständig computerüberwacht, so daß die Aufnahmen verschiedener Kameras auf einem Computerbildschirm angezeigt werden, interaktive Audio-/Video-Verbindungen aufgebaut werden können usw. Der Vorteil dieses Systems besteht darin, daß es zu verstärkter Verständigung der Beteiligten darüber führt, wer anwesend ist, welche Art von Tätigkeiten ausgeführt werden, ob jemand beschäftigt ist. Diese Technologie wird der Prototyp vieler kommerzieller Produkte sein, die auf große Märkte zielen. Ohne jegliche Einrichtung zum Schutz der Privatsphäre führt diese Technologie zu einer ernsthaften Gefährdung für die Privatsphäre des Benutzers.

Diese Technologie könnte zu einer unbemerkten, kombinierten Audio-, Video- und Computerbeobachtung führen, die die Leistung der Arbeitnehmer am Ar-

beitsplatz überwacht. Diese Einrichtungen könnten einem unethischen Gebrauch von Technologie Vorschub leisten und darüber hinaus dem versehentlichen Eindringen in die Privatsphäre förderlich sein. Es entwickelt sich jedoch eine ganz neue Klasse von Datenschutzproblemen in Verbindung mit verschiedenen Befürchtungen über einen schnell wachsenden, bisher unbekannten Problemkreis, der sich aus dem Zusammenhang zwischen Benutzerschnittstellendesign und sozialem Verhalten entwickelt. Entkörperlichung (etwa wenn nur ein Gesicht oder nur der Name und die Stimme auf dem Bildschirm dargestellt werden) kann entstehen aus dem Zusammenhang, in den hinein oder aus dem heraus Informationen vermittelt werden; dadurch werden die Handlungen des Betroffenen aus diesem Zusammenhang gerissen. Das Fehlen einer Rückmeldung über das eigene Verhalten, wie die unbewußt wahrgenommenen Signale der Körpersprache des Kommunikationspartners oder der benutzten Technologie kann dazu führen, daß man sicht nicht bewußt ist, wann und welche Informationen man über sich selbst übermittelt.

Gleichartige Entkörperlichungseffekte treten im Zusammenhang mit Telefon- und E-Mail-Verbindungen auf, ohne jedoch bisher viel Aufmerksamkeit erregt zu haben. Kontextverlust tritt auf, wenn nur die Ergebnisse von Handlungen ohne das Wissen darüber, wie diese Ergebnisse erreicht wurde, mitgeteilt werden. All dies kann negative Auswirkungen auf das soziale Verhalten haben.

Der Datenschutz des Einzelnen steht im Zusammenhang mit Aspekten der Technik- und Benutzerschnittstellenentwicklung der benutzten Technologie. Besucher von Orten, an denen „media spaces“ mit einer kontinuierlichen Kontrolle benutzt wurden, waren mit ihrer Fähigkeit, ihre Selbstpräsentation und damit ihre Privatsphäre zu überwachen und zu kontrollieren, unzufrieden. Während längerdauernder Ton- und Bildverbindungen neigen Personen dazu, deren Existenz und die damit zusammenhängenden Auswirkungen zu vergessen.

II. Empfehlungen

1. Einbeziehung der Arbeitnehmervertretung

Die Arbeitnehmervertretung sollte im Vorfeld jeglicher Entscheidungen über die Einführung und Nutzung von Informationstechnologien und Telekommunikation zur Aufzeichnung von Informationen am Arbeitsplatz in vollem Umfang informiert und um Stellungnahme gebeten werden. Sie muß jederzeit in der Lage sein zu überprüfen, ob Bestimmungen und Richtlinien über den Datenschutz der Arbeitnehmer eingehalten werden. Diese Befugnis zur Überprüfung ist in dem Maße eingeschränkt, wie sie selbst zu einer Verletzung des Datenschutzes von Arbeitnehmern führen würde. Die Information und Beratung muß die Gründe und die Notwendigkeit der Einführung des neuen Datenaufzeichnungssystems, die

Angemessenheit der vorgeschlagenen Technologie, die Funktion der Technologie, die Art der aufgezeichneten Daten und in welchem Umfang diese aufgezeichnet werden, die Personen, an die diese Daten weitergegeben werden, und die Rechte der Arbeitnehmer enthalten. Einschneidende Veränderungen in der Struktur der benutzten Informationstechnologie am Arbeitsplatz sollten nur mit der Zustimmung der Arbeitnehmervertretung vorgenommen werden.

2. Information der Arbeitnehmer

Vor der Einführung und Nutzung von Informationstechnologien oder Telekommunikation am Arbeitsplatz zur Aufzeichnung von Daten sollten die Arbeitnehmer über die Gründe, aus denen diese Daten erforderlich sind, die Zwecke, für die sie verwandt werden, die Funktionen der für die Aufzeichnung der Daten benutzten Technologie, die Art der aufgezeichneten Daten, die Personen, an die diese Daten weitergegeben werden können und über ihre eigenen Rechte, die über sie verarbeiteten Daten einzusehen und Fehler zu korrigieren, informiert werden. Die Rechte auf Einsicht und Berichtigung müssen innerhalb einer angemessenen Zeitspanne wahrgenommen werden können.

Der Arbeitgeber muß seine Angestellten über seine Politik hinsichtlich der Nutzung von Informationstechnologie am Arbeitsplatz (z. B. elektronische Post oder voice mail) unterrichten. Er sollte sie außerdem darüber informieren, zu welchen primären und sekundären Zwecken die von solchen Systemen aufgezeichneten personenbezogenen Daten genutzt werden.

3. Beachtung der berechtigten Erwartung der Arbeitnehmer im Hinblick auf den Datenschutz

Die Speicherung von Daten muß auf das Prinzip der Respektierung der „legitimen Erwartung des Arbeitnehmers im Hinblick auf den Datenschutz“ gestützt werden.

Der legitime Charakter der Erwartung eines Arbeitnehmers muß im Zusammenhang mit den spezifischen Gegebenheiten der jeweiligen Situation analysiert werden.

Die Erwartung des Arbeitnehmers im Hinblick auf den Datenschutz wird an räumlich abgeschlossenen Arbeitsplätzen höher sein als an Arbeitsplätzen, die von anderen eingesehen werden können. Sie werden andererseits abgewogen werden müssen gegen Sicherheitsanforderungen an solchen Arbeitsplätzen, an denen regelmäßig umfangreiche Sicherheitsmaßnahmen getroffen werden.

4. Zweckbindungsprinzip

Informationstechnologie und Telekommunikation darf am Arbeitsplatz zur Speicherung, Nutzung und Übermittlung von Daten für vordefinierte gesetzmäßige und legitime Zwecke genutzt werden.

Die Zwecke der Verarbeitung personenbezogener Daten über die Arbeitnehmer dürfen nicht gegen Treu und Glauben verstoßen oder die Menschenwürde beeinträchtigen. Sie müssen notwendig, verhältnismäßig und der vertrauensvollen Zusammenarbeit, von der berufliche Beziehungen bestimmt sein sollten, angemessen sein.

Die Daten sollten im Hinblick auf die Zwecke, zu denen sie gespeichert werden, erforderlich, relevant, angemessen und vom Umfang her nicht unverhältnismäßig sein.

In Fällen, in denen Maschinen aus Sicherheitsgründen durch Kameras überwacht werden müssen, kann es unverhältnismäßig sein, die Überwachung auf die an den Maschinen beschäftigten Personen auszudehnen.

Dort, wo „Badge-Systeme“ zur Kontrolle des Zugangs zum Arbeitsplatz eingesetzt werden, kann es unzulässig sein, diese Badge-Leser an ein zentrales Registrierungssystem anzuschließen. Die entstehenden Daten dürfen nur insofern und so lange gespeichert werden, wie sie für relevant und notwendig für die Realisierung der beschriebenen Zwecke gelten können.

5. Beschränkung der Speicherung personenbezogener Daten über Arbeitnehmer

Bei der Einführung oder Nutzung von Informationstechnologie oder Telekommunikation am Arbeitsplatz zur Erhebung von Daten sollte der Arbeitgeber von der Speicherung personenbezogener Daten, die keinen direkten Bezug zum Arbeitsverhältnis haben, wie das persönliche Verhalten, persönliche Eigenschaften sowie auch persönliche interne oder externe Beziehungen der Arbeitnehmer absehen.

6. Verwendung personenbezogener Daten gegen einen einzelnen Arbeitnehmer

Informationen, die durch die Nutzung von Informationstechnologie oder Telekommunikation erhoben worden sind, dürfen nicht gegen einen Arbeitnehmer verwendet werden, wenn dieser nicht vorher gemäß Empfehlung 2 unterrichtet worden ist. Die erhobenen Informationen dürfen nur gegen einen Arbeitnehmer verwendet werden, nachdem er die Gelegenheit hatte, die Informationen einzusehen und sie zu überprüfen.

7. Verdeckte Überwachung einzelner Arbeitnehmer

Die Speicherung oder der Zugriff des Arbeitgebers auf personenbezogene Daten über den Arbeitnehmer ohne vorherige Mitteilung oder für andere Zwecke als angegeben kann nur unter außergewöhnlichen Umständen gerechtfertigt sein. Dies setzt einen begründeten Verdacht voraus, daß eine schwerwiegende Straftat begangen wurde oder begangen werden soll.

Die Informationen dürfen nur dann gespeichert oder verwendet werden, wenn eine von den Verantwortlichen unterschriebene, schriftliche Anweisung vorliegt. Diese schriftliche Anweisung muß enthalten:

- die Anhaltspunkte für den begründeten Verdacht, daß eine schwerwiegende Straftat begangen wird, begangen wurde oder begangen werden soll,

- die Gründe, aus denen die Speicherung von oder der Zugriff auf personenbezogene Daten über einen Arbeitnehmer erforderlich ist,

- die Art der erhobenen Informationen.

Die erhobene Information darf in jedem Fall nur im Einklang mit Empfehlung 6 (s. oben) verwendet werden.

Die Arbeitnehmervertretung ist zu informieren.

8. Notwendigkeit einer überwachungsfreien Zone

Der Arbeitgeber muß im Betrieb einen angemessenen Bereich vorsehen, in dem die Privatsphäre der Arbeitnehmer garantiert wird, in dem eine unbeobachtete Kommunikation mit anderen Personen möglich ist und in dem Telekommunikationseinrichtungen zum Senden oder zum Empfang persönlicher Nachrichten zur Verfügung stehen.

III. Einzelne Technologien

Die Bedeutung der oben gegebenen Empfehlungen soll durch drei Beispiele neuer technologischer Entwicklungen illustriert werden, die bereits jetzt oder in naher Zukunft sowohl im privaten als auch im öffentlichen Sektor genutzt werden.

1. Medialer Raum

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation gibt im Hinblick auf mediale Räume die folgenden Empfehlungen:

1.1 Kontrolle und Rückmeldung

Es besteht eine Notwendigkeit für eine Kontrolle und Rückmeldung über die in dem allgegenwärtigen Computersystem enthaltenen Informationen, da es hier keine der Signale gibt, die normalerweise bei persönlichen Treffen wahrgenommen werden können. Kontrolle und Rückmeldung müssen in jeder Phase des Kommunikationsprozesses angewandt werden. Ohne Kontrolle und Rückmeldung kann den Nutzern des medialen Raums die Furcht vor der Verletzung ihrer Privatsphäre nicht genommen werden.

1.1.1 Kontrolle

Kontrolle bedeutet, „Personen in die Lage zu versetzen, Einfluß darauf auszuüben, welche Informationen sie weitergeben und wer diese erhalten kann". Kontrolle impliziert auch, daß der Nutzer eines medialen Raums festlegen kann, wer sich mit ihm in Verbindung setzen kann und welche Verbindungen den einzelnen Personen erlaubt sind.Beteiligt sich ein Nutzer nicht aktiv, so muß das System dies als automatische Ablehnung der Kontaktaufnahme mit anderen interpretieren.

Hier sollten vier Datenschutzaspekte in Betracht gezogen werden, nämlich

– die Kontrolle darüber, wer den Benutzer zu einer bestimmten Zeit sehen oder hören kann;

– die Information des Nutzers, wenn ihn jemand tatsächlich sieht oder hört;

– die Information über den Zweck dieser Verbindung und

– die Verhinderung von Verbindungen, die die Arbeit des Benutzers stören.

Verbindungen dürfen nicht ohne die Einwilligung des Benutzers aufgebaut werden.

1.1.2 Rückmeldung und Gegenseitigkeit

Rückmeldung bedeutet die Information darüber, wann welche Informationen über jemanden aufgezeichnet werden und wem diese Information zur Verfügung gestellt wird. Die Art der Rückmeldung hängt von der Art der Verbindung ab. Je mehr Interaktion notwendig ist, desto mehr Gegenseitigkeit sollte erforderlich sein (wenn ich dich sehen kann, kannst du mich auch sehen). In dem Augenblick, in dem eine Verbindung aufgebaut wird, sollte ein Warnsignal auf dem Bildschirm angezeigt und ein akustisches Signal gegeben werden.

1.2 Gestaltungsanforderungen

Die Empfehlung, daß Koltroll-, Rückmeldungs- und Gegenseitigkeitsmechanismen in allgegenwärtigen Computersystemen enthalten sein müssen, ist der einzige Weg, den Datenschutz sicherzustellen und zu verhindern, daß Aufzeichnungen über unsere Aktivitäten aufbewahrt, unter Umständen verändert und zu einem späteren Zeitpunkt außerhalb ihres ursprünglichen Kontexts verwendet werden können.

1.2.1 Erforderlichkeit

Weiterhin ist es notwendig zu wissen, was mit den gesammelten Informationen geschieht (werden sie verschlüsselt, verarbeitet, gespeichert, wenn ja, in welcher Form), wer auf diese Informationen zugreifen kann (jeder, bestimmte Gruppen, bestimmte Personen, nur man selbst) und zu welchen Zwecken die Information genutzt wird und zukünftig genutzt werden soll. Die Gewährung eines unveräußerlichen Rechts des Einzelnen auf informationelle Selbstbestimmung ist entscheidend, wie das Deutsche Bundesverfassungsgericht 1983 ausgeführt hat.

1.2.2 Entwurfskriterien

Basierend auf der Feststellung, daß Kontrolle, Rückmeldung und Gegenseitigkeit bei der Sammlung von Informationen durch und über den Einzelnen und Datensicherheit unabdingbar sind, um die Beeinträchtigung des Datenschutzes zu verhindern, kann man zumindest vier Entwurfskriterien ausfindig machen:

e) aKontrolle,

f) Rückmeldung

g) Datensicherheit und

h) Optionen, um die Speicherung der Daten insgesamt zu verhindern,

die bei jedem Entwurf eines Produktes oder Dienstes im Lichte des fundamentalen Rechts des Einzelnen, darüber zu entscheiden, wann und unter welchen Umständen seine personenbezogenen Daten offenbart werden dürfen, berücksichtigt werden sollten.

Das vierte Kriterium (d) wirft die Frage auf, ob die gewünschte Funktionalität durch ein System erreicht werden kann, in dem der Betroffene selbst sicherstellen kann, daß datenschutzrelevante Informationen, die in das System eingegeben werden, nicht anderen zugänglich gewesen sind. Die Niederländische Daten-

schutzbehörde hat einen Bericht über datenschutzfreundliche Technologien veröffentlicht, der beweist, daß solche Technologien in jeder Arbeitsplatzumgebung angewendet werden können.

2. Telearbeit

Wenn der Arbeitnehmer seine Arbeit in seiner privaten Wohnung ausführt, ist der Arbeitgeber nicht berechtigt, Aufzeichnungsgeräte zu installieren, wenn er nicht garantieren kann, daß nur solche Daten verarbeitet werden, die in enger Verbindung mit der beruflichen Tätigkeit des Arbeitnehmers stehen. Falls der Arbeitnehmer mit der Einwilligung des Arbeitgebers einen Computer sowohl für die Telearbeit als auch für private Zwecke nutzt, müssen die privaten Daten des Arbeitnehmers effizient gegen jegliche Kenntnisnahme durch den Arbeitgeber geschützt werden. Andererseits muß der Arbeitnehmer für einen effektiven Schutz dagegen sorgen, daß Angehörige seines Haushalts bei der Telearbeit verarbeitete personenbezogene Daten absichtlich oder zufällig zur Kenntnis nehmen können.

Die Probleme, die insbesondere bei grenzüberschreitender Telearbeit entstehen, müssen noch genauer untersucht werden. Die Arbeitsgruppe wird die weiteren Entwicklungen in diesem Bereich beobachten.

3. Veröffentlichung von Arbeitnehmerdaten in elektronischen Verzeichnissen

Die Arbeitsgruppe verweist auf ihren Bericht an die 13. Internationale Konferenz der Datenschutzbeauftragten von 1991, in dem sie die aus der Nutzung von elektronischen Verzeichnissen (z. B. X. 500) entstehenden Probleme hervorgehoben hat. Nach erneuter Überprüfung der in diesem Bericht aufgestellten Prinzipien vertritt die Arbeitsgruppe die Auffassung, daß zwischen Daten, deren Übermittlung aus bestimmten beruflichen Anforderungen erforderlich ist (z. B. in der Wissenschaft), und anderen Daten unterschieden werden muß.

Basiskommunikationsdaten des Arbeitnehmers (z. B. Postadresse, E-Mail-Adresse usw.) können ohne die Einwilligung des Arbeitnehmers in elektronische Verzeichnisse aufgenommen werden, wenn hierfür eine arbeitsvertragliche Notwendigkeit besteht. Andere (zusätzliche) Daten dürfen nur mit der Zustimmung des Arbeitnehmers in dem Verzeichnis veröffentlicht werden, vorausgesetzt, daß diese Daten in Beziehung zu der beruflichen Tätigkeit des Arbeitnehmers stehen (spezielle Interessengebiete; Veröffentlichungen usw.).

In jedem Fall muß der Arbeitgeber die Arbeitnehmer gründlich und umfassend über die Art der in das Verzeichnis aufgenommenen Daten informieren sowie darüber, ob sie ihr Einverständnis für bestimmte Einträge im Hinblick auf die oben getroffene Unterscheidung verweigern können und welche Konsequenzen eine

Verweigerung haben kann. Die Arbeitnehmer müssen ein Recht auf Einsicht in die über sie gespeicherten Daten haben sowie das Recht, ihre Daten im Bedarfsfall korrigieren zu lassen und ihre Einwilligung zurückzuziehen.

Report and Recommendations on Telecommunications and Privacy in Labour Relationships (August 1996)

Preliminary note

The object of this paper is to provide for a number of recommendations regarding information technologies and telecommunications when being used at the workplace to generate information concerning the workers.

Their use has drastically changed und multiplied the methods to collect and process information at the workplace. Continuous supervision and collection of data concerning different aspects of the worker's activities, possibly without their knowledge, is feasible**.** The availability of these new methods becomes more general and they gradually gain acceptance at the workplace.They are implemented for security reasons, for controlling and allocating costs of different performances and communications, to measure and improve productivity. They however hold an enormous potential of collecting and processing data on the worker's personal behaviour, activities and characteristics. The risks of intrusions on the worker's privacy are enormous and therefore need to be taken into consideration from a data protection approach.

The notion of "workplace" when used in this context must be understood in a wide sense as any place where the worker is located when performing work by order of his employer. This can be the employers' sites, as well as the workers' vehicule or his private residence. In this regard, the recent developments towards teleworking deserve special attention.

The first part of the paper gives a survey of the data collection methods based on information technologies and telecommunications that are used at the workplace, and of their potential to generate information on the employees.

In a second part, a number of recommendations are given as to the respect of privacy at the workplace. In the first place some procedural conditions are formulated to be respected when implementing data recording devices at the workplace. Secondly, substance is given to the right of privacy of the worker.

In a third and final part three specific applications of these recommendations to information technologies and telecommunications are described.

In this context, it must be mentioned that a Recommendation No. R (89)2 of the Committee of Ministers to Member States of the Council of Europe on the protection of personal data used for employment purposes was adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies. The principles set out in this Recommendation apply specifically to the collection and use of personal data for employment purposes in public and private sectors.

Furthermore, the International Labour Organisation is currently discussing a draft Code of practice on workers' privacy.

Finally, the question of the protection of personal data at the workplace is currently being taken into consideration by the DG V of the European Commission.

The recommendations set out hereafter specifically focus on the implementation and the use of telecommunications and information technologies to collect and process information on workers. Their fast growing acceptance at the workplace, their enormous potential to collect and process personal data for different purposes make it necessary to take them into consideration from a privacy point of view. Given the current lack of regulation in this area, a set of recommendations could be a useful tool for employers willing to respect the rules concerning the protection of personal data at the workplace.

I. Methods of data collection and processing based on information technologies and telecommunications

1. A wide range of data recording devices based on the use of computers, telecommunications or audio-visual technologies gain acceptance at the workplace:

   – Active badges (badge systems) (also called „tabs" or more neutrally „network location devices") about a few inches big developed for example by Olivetti and Bellcore containing a microprocessor and infrared transmitters broadcast the identity of its wearer and trigger all kinds of responses from other ICT devices like automatic telephone forwarding, authorizing the access to buildings and meeting rooms and all kinds of other convenience. These systems could cause a lot of trouble for the wearer in the wrong hands, especially when connected to a central computer system to collect data on the arrivals and departures of the workers. Within the buildings, they record the moves of the workers (to libraries, restrooms, different workstations, etc.) and the time they spent in each area of the buildings; badge systems based on the recognition of biometric identifiers (such as fingerprints) pose in themselves privacy risks given the collection and the retention of these identifiers.

– computer-based systems used by the employers provide information on the work-rhythm by recording the time needed to fulfill a transaction, or the numer of tasks performed over a period (e.g. counting keystrokes, number of errors, lenghts of breaks, etc.). Aside from use-monitoring, computers systems can be used for remote access to a worker's files and e-mail correspondence, as well as the remote mirroring of the workers' actions. Project management or work flow automation software developed as a productivity enhancer may impede the right to privacy of users because of its potential to eavesdropping on the employee.

– video-cameras placed for safety reasons at entrances or in places requiring a high level of security record personal data on the workers, such as work habits, behaviour, contacts with colleagues, as well as on persons other than the workers.

– telephone-call accounting systems record time and duration of incoming and outgoing, internal and external calls; in addition telephone monitoring record the numbers of calling or called third persons as well as the content of professional and private conversations; with regard to other telecommunications, such as electronic mail, means can also be used for generating data on the workers' internal or external communication.

– the introduction of computers and the extension of network-based or satellite communications devices at the homes, in the vehicles, (e. o.) allow for remote control of workers far beyond the sites of the employer.

– telework is a catalyst for the computerization of the private homes of the workers and for the extension of network-based or satellite communications devices towards these private residences. They are implemented to create a professional environment outside the employers' sites and to facilitate communications between workers. Satellite technologies for mobile telephone allow to keep track of the location of the worker outside the firm.

2. Privacy intrusion is a function of capability of technology and attitude of people. The following enumeration shows some features of the control possibilities offered by the information technologies and telecommunications and of their invasive character of the privacy of the workers.

– The new technologies allow for the creation of increasing and more sophisticated information sources on workers. They hold unprecedented potential to gather, to measure and to evaluate a wide range of information not only on performances of the worker, but also on his personal characteristics, his behaviour, his relations with colleagues and even with third parties from outside the workplace;

– the new information technologies allow for continuous monitoring and surveillance at the workplace. In certain cases, information on the workers' performance or personal behaviour can be gathered and used secretly or for purposes the workers are not aware of;

– the evolution towards telework probably holds the most important risk of intrusions into the privacy of the worker. The physical distance between the employer and the workers, as well as between the workers themselves, will be a catalyst for the implementation of data recording devices, thus allowing for remote control by the employer. This poses in itself a risk to the privacy. Furthermore, as the boundaries between professional and private life fade, any inappropriate use of the recording devices in a telework context may allow for the processing of very different types of personal data that have no direct connection or no connection at all with the professional relationship.

– A new kind of technology which has the potential of pivacy intrusion is the development of media spaces. A media space is a computer-controlled network of audiovideo equipment used to support communication and collaboration between people within a group separated by architecture in a building and by geographical distance through nodes.

Every room has several audio and video cables running to and from a central switch as well as an access to digital networks. The resulting system provides all rooms with some form of an audio-video "node" consisting of a camera, monitor, microphone and speakers. The connections between the nodes are completely computercontrolled, so that people can display the views from various cameras on their desktop monitors, set up two-way audio-video connections etc. The advantage of this system is that it promotes focussed collaboration between the participants about who is around, what sort of things they are doing, whether they are busy and so on. This technology will be the forerunner of many commercial products aimed at wide markets. Without any privacy protection features this technology poses seriuous threats of intrusion into the user's privacy.

This technology may lead to an unnoticed combined audio, video and computer surveillance, monitoring the worker's performance on the job. These features may foster unethical use of technology but, more significantly, they are also much more conducive to inadvertent intrusions on privacy. But a new class of privacy problerns emerges which is related to very different concerns about a fast growing, less well understood set of issues arising from user-interface design features which interfere with social behaviour. Disembodiment (for example only a face is seen on the monitor, or only your name may be presented on the screen with your voice only) may occur from the context into and from which one projects information and dissociation from one's actions may happen. The lack of feed-

back on one's own behaviour, like the unconsciously noted body-language cues from the one with whom you are communicating or from the used technology may lead to unawareness what and when you are conveying information about yourself.

Similar disembodiment effects occur in the context of telephone and e-mail conversations, but did not draw very much attention so far. Dissociation occurs when only the results of actions are shared not knowing who did what to reach the results. This all may have negative effects on social behaviour.

Privacy of the individual interacts with the technical and interface design aspects of the technology they use. Visitors to places where media spaces were used with a moment-to-moment continuous control felt uneasy about their ability to monitor and control their self-presentation and consequently their privacy. During extended durations of audio/video connection peopie tend to forget about their existence and associated implications.

II. Recommendations

1. Workers' representatives involvement

The workers' representatives must be fully informed and consulted prior to any decision to introduce and use information technologies and telecommunications to generate information at the workplace. They must be able at any time to check whether regulations and guidelines to protect the workers' privacy are complied with. This checking ability is restricted insofar as doing so would in itself invade an employee's privacy. The information and consultation must bear on the reasons and the need for the introduction of the new data record system, the appropriateness of the proposed technology, the features of the technology, the nature of the data recorded and the extent to which they are recorded, the persons to which they are disclosed, and the workers' rights. Fundamental changes in the structure of information technology in use at the workplace should only be made with the consent of the workers' representatives.

2. Information of the workers

Where information technologies or telecommunications are implemented and used at the workplace to generate data, the workers must prior be informed on the reasons for which these data are needed and the purposes for which they are used, the features of the technology used to generate the data, the nature of the generated data, the persons to which these data might be disclosed, their rights to have access to the data processed about him and to correct errors. The rights to have access and to correct must be ensured within a reasonable period of time.

The employer has to inform his employees about the policy on the use of information technology (e.g. electronic mail or voice mail) at the workplace. He should also inform them about the principal and secondary uses to which the personal data generated by such systems are being put.

3. Respect of the workers' reasonable expectations of privacy

The collection of data must be based on the principle of respect for the "workers' legitimate expectations of privacy".

The legitimate character of a workers' expectation must be analysed according to the specific facts of the situation.

The workers' expectations of privacy will be higher in case of closed workplaces than in workplaces open to others. On the other hand they will have to be harmonized with security needs in places where extreme security measures are regularly taken.

4. Finality principle

Information technologies and telecommunications can only be used at the workplace to collect, use and disclose data for predefined lawful and legitimate purposes.

The finality of the processing of the workers' privacy shall not be unfair and affect human dignity. lt must be necessary, proportionate and adequate to the good faith that should reign professional relations.

Data should be necessary, relevant, adequate and not excessive given the finality for which they are collected.

Where for security reasons machines are to be surveilled by cameras, it may be excessive to extend the surveillance to the persons working at the machines.

Where badge systems are implemented in order to control the access to the workplaces, it may be aberrant to interconnect these badge readers to a central registration system. Data generated can only be stored in so far and for so long as they can be considered to be relevant and necessary for the realisation of the described purposes.

5. Restraint of collection of personal data concerning the worker

When implementing or using information technologies or telecommunications at the workplace to generate data, the employer should refrain from collecting per-

sonal data that are not directly relevant within the professional reiationship such as the personal behaviour, personal characteristics as well as the personal internal and external contacts of the worker.

6. Use of personal data against an individual worker

No information generated by the use of an information technology or telecommunications may be used against a worker if the latter has not previously received the information mentioned in point 2. The information generated may only be used against the worker after he has had the opportunity to have access to this information and to challenge it.

7. Covert surveillance of an individual worker

Only exceptional circumstances may justify the employer's collection of or access to personal data concerning the employee without prior notice, or for other purposes than the purposes described. This requires that there is a serious suspicion that a grievous criminal activity has been or will be committed.

The information can only be collected or accessed to when a written statement, signed by the authorised person can be produced. This written statement must explain:

– the reasons why there is a serious suspicion that a grievous criminal activity is, has been or will be committed,

– the reasons why collection or access to personal data concerning an employee is necessary,

– the nature of the information gathered.

In any case the gathered information may only be used in accordance with Recommendation 6 (above).

Organisations of workers shall be informed.

8. Need for a surveillance-free zone

The employer must assure that there is an appropriate zone where the privacy of the worker is guaranteed, where free communication with other persons is possible, where they have telecommunications means for sending or receiving personal messages at their disposal.

III. Specific technologies

The importance of the recommendations given above may be illustrated by three examples of new technological developments which are already in use or will be used in the private as well as the public sector very soon.

1. Media Space

The International Working Group on Data Protection in Telecommunications recommend the following recommendations concerning media space:

1.1 Control and feedback

What is needed is control and feedback of information captured in the ubiquitous computing environments, as there are no cues available which normally are noticeable in face-to-face meetings and have to be applied to each phase of the communication process. Without control and feedback the fear of the media space users of privacy intrusion can't be taken away from them.

1.1.1 Control

Control is "empowering people to stipulate what information they project and who can get hold of it." Control also implies that the user of the media space determines who may connect to him and what connections each person is allowed to make. No action from the user is interpreted by the system as an automatic rejection of connections with others.

We should take into consideration four privacy aspects, namely

– control over who can see and hear the user at a given time;

– knowledge of when somebody is in fact seeing or hearing the user;

– knowledge of the intention behind the connection and

– to avoid connections being intrusions on the work of the user.

No connections may be made without the permission of the user.

1.1.2 Feedback and reciprocity

Feedback is informing people when and what information about them is being captured and to whom the information is being made available. Feedback depends on the type of the connection made. The more interaction is needed, the more

reciprocity (if I can see you, you can see me) should be required. At the moment a connection is made a warning signal should be displayed on the screen and an audio signal should be given.

1.2 Design requirements

The recommendation that control, feedback and reciprocity mechanisms have to be built-in in an ubiquitous computing environment is the only way to safeguard privacy and prevents that potential records of our activity may be kept and possibly manipulated and used at a later date and out of their original context.

1.2.1 Need to know

Further it is necessary to know what happens to the information gathered (is it encrypted, processed, stored, in what form), to whom is this information accessible (public, particular groups, certain persons, only oneself) and to what uses is the present information put and how it might be used in the future. lt is essential that the individual has an unalienable right to information self-determination, as has been pointed out in 1983 by the German Constitutional Court.

1.2.2 Design criteria

Based on the findings that control, feedback and reciprocity of the information capture by the individual and data security is crucial to prevent privacy intrusions, there are at least four design criteria:

a) control,

b) feedback,

c) data security and

d) means to prevent the collection of the data altogether,

which should be taken into consideration whenever designing a product or service, all in the light of the fundamental right of the individuals to decide when and under what circumstances their personal data may be revealed.

The fourth criterion (d) questions whether the required functionality can be achieved by a system where the data subject itself can verify that the privacy-related data that form the input of the system have not been available to someone else. The Dutch Data Protection Authority has issued a report on privacy-enhancing technologies which proves that such technology can be applied in any workplace environment.

2. Telework

When the worker is performing work at his private home, the employer is not entitled to install any recording devices unless he can guarantee that only data closely related to the employee's professional activities are processed. In case the employee uses a computer for telework as well as for private purposes with the employer's permission, the employee's private data must be effectively protected against inspection by the employer. On the other hand the employee has to provide for effective protection against members of his household inspecting or accidentally looking into personal data processed for telework purposes.

The problems related to telework especially in a transborder situation need a study in greater depth. The Working Group will monitor developments in this field closely.

3. Communication of employee data by means of electronic directories

The Working Group refers to its Report to the 13th International Conference of Data Protection Commissioners in 1991 where it highlighted the privacy issues arising from the use of electronic directories (e. g. X. 500). Having reconsidered the principles set out in this Report the Working Groups takes the view that a distinction has to be made between data the communication of which is required by the particular professional requirements (e. g. in the scientific community) and other data.

The employee's basic communication parameters (e. g. postal address, e-mail address etc.) may be transmitted via an electronic directory without the employee's consent insofar as the contract of employment requires the entry in the directory. Other (additional) data may only be published in the directory with the consent of the employee concerned provided that these data are related to the employee's profession (special areas of interest; publications etc.).

In general the employer has to inform the employees thoroughly and comprehensibly about the range of data which are entered in the directory, if they can refuse to agree with an entry according to the distinction just made and what consequences a refusal may have. The employees must have the right to inspect their data, to correct them if necessary and to revoke their consent, as the case may be.

1997

Gemeinsame Erklärung über Kryptographie – 12. September 1997 –

Der Schutz der persönlichen Kommunikation vor willkürlichen Eingriffen ist ein Menschenrecht (Art. 12 Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948; Art. 17 des Internationalen Paktes über Bürger- und politische Rechte; Art. 8 der Europäischen Menschenrechtskonvention). In der Informationsgesellschaft, in der die Kommunikation überwiegend mit den Mitteln der Telekommunikation stattfindet, bedeutet dieses Recht, daß jeder einen Anspruch darauf hat, daß seine elektronisch übermittelten Mitteilungen vertraulich behandelt werden und kein Unbefugter den Inhalt wahrnehmen kann.

Auf Vorschlag der Internationalen Arbeitsgruppe Telekommunikation und Medien hat die 7. Internationale Konferenz der Datenschutzbeauftragten auf ihrer Sitzung in Luxemburg am 26. September 1985 in einem Beschluß darauf hingewiesen, daß Integration und Digitalisierung die Gefahr des unbefugten Aufzeichnens und Auswertens der übermittelten Informationen erhöhen. Die 11. Internationale Konferenz der Datenschutzbeauftragten hat auf ihrer Sitzung am 30. August 1989 in Berlin gefordert, Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören und zur Gewährleistung der Authentizität des Senders auf höchstem technischen Niveau und zu akzeptablen Preisen anzubieten.

Das einzige diesen Anforderungen entsprechende Mittel ist die Verschlüsselung der Nachrichten. Das Angebot ausreichender Verschlüsselungsmethoden an die Teilnehmer der Telekommunikation ist damit eine elementare Forderung zur Sicherstellung des Datenschutzes. Es bildet darüber hinaus die Grundlage für datenschutzfreundliche Technologien. Für den Mobilfunk hat die 12. Internationale Konferenz der Datenschutzbeauftragten auf ihrer Sitzung in Paris am 19. September 1990 gefordert, Netzbetreiber sollten verpflichtet sein, den Teilnehmern wirksame Verschlüsselungsverfahren anzubieten. Das Angebot einer end-to-end-Verschlüsselung war eine wesentliche Forderung der Datenschutzbeauftragten bei der Diskussion über den Entwurf einer Richtlinie des Rates der Europäischen Union zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation bekräftigt ihre Forderung, daß zur Sicherstellung der Vertraulichkeit jedem Teilnehmer elektronischer Telekommunikationsdienste ermöglicht werden muß, seine Nachrichten auf einem von ihm zu frei wählenden Niveau zu verschlüsseln.

Das in einigen Ländern erörterte Verbot der Verschlüsselung von Nachrichten widerspricht diesem Grundsatz. Es behindert die Bürger nicht nur bei der Wahrnehmung ihres Menschenrechts auf unbeobachtbare Kommunikation, sondern fördert den Mißbrauch der Telekommunikation für illegale Zwecke. Es kann von denjenigen, die über entsprechende technische und finanzielle Mittel verfügen, jederzeit umgangen werden, so daß ein Verbot nur den arglosen Bürger trifft.

Auch eine Beschränkung der Möglichkeiten zur Verschlüsselung zum Beispiel durch Lizensierung der erforderlichen Software hätte diesen Effekt. Sie ist aus den genannten Gründen insbesondere nicht geeignet, die organisierte Kriminalität zu bekämpfen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat Verständnis für die Bedürfnisse der Sicherheitsbehörden, bei der Gefahrenabwehr und der Strafverfolgung auch auf verschlüsselte Nachrichten zugreifen zu können. Die 14. Internationale Konferenz der Datenschutzbeauftragten in Sydney am 29. Oktober 1992 hat einen ausführlichen Bericht der Arbeitsgruppe über die Problematik des Zugriffs von Sicherheitsbehörden auf die Telekommunikation zustimmend zur Kenntnis genommen. Die Konferenz stimmte darin überein, daß die technische und rechtliche Entwicklung im Bereich des Fernmeldegeheimnisses sorgfältig beobachtet werden muß, um die Privatsphäre des Einzelnen vor exzessiver Überwachung zu schützen.

Die Arbeitsgruppe bezweifelt, daß eine Regulierung der Verschlüsselung zugunsten der Sicherheitsbehörden einen angemessenen Beitrag zur Bekämpfung der schweren Kriminalität leisten kann. Für die Bekämpfung von Straftaten geringerer Schwere wäre ein Eingriff in das Telekommunikationsgeheimnis ohnehin unverhältnismäßig. Alle erörterten Modelle (Lizensierung der Software, Ex- und Importbeschränkungen, Schlüsselhinterlegung, hardwareseitige Hintertüren wie „clipper chip“) führen zu einem schwächeren Schutz, da diese Lösungen auch unbefugt genutzt werden können. Die Durchsetzung gesetzlicher Verpflichtungen, nur bestimmte, lizensierte Schlüssel zu benutzen, würde das Verhältnis von genereller Vertraulichkeit und ausnahmsweise gesetzlich erlaubtem Zugriff umkehren. Da alle entsprechenden gesetzlichen Verpflichtungen mit ausreichenden technischen und finanziellen Mitteln (z. B. durch Verbergen der Verschlüsselung – Steganografie) umgangen werden können, würde dies zu einer unverhältnismäßigen und letztendlich nutzlosen Überwachung des Einzelnen führen. Daher gibt es einen Unterschied zwischen Eingiffen in traditionelle Formen der Korrespondenz und deren elektronischer Übertragung: Eingriffe in die erstgenannte Form der Kommunikation können legal sein, wenn es „… in einer demokratischen Gesellschaft zur Bekämpfung von Störungen der öffentlichen Ordnung und Verbrechen notwendig ist …“ (Art. 8 Abs. 2 Europäische Menschenrechtskonvention); Eingriffe in die elektronische Kommunikation zur Durchsetzung der Limitierung

von krypographischen Methoden können zur Abschaffung vertraulicher elektronischer Kommunikation insgesamt führen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation begrüßt sowohl die OECD-Leitlinien über Kryptographie-Politik vom 27. März 1997 als auch die Gemeinsame Erklärung der Europäischen Ministerkonferenz (Bonn, 6.–8. Juli 1997), in denen die Bedeutung vertrauenswürdiger kryptographischer Methoden zur Erreichung des Vertrauens der Benutzer in verläßliche Informations- und Kommunikationssysteme betont wird. Die OECD-Leitlinien betonen darüber hinaus das Prinzip, daß die freie Auswahl des Benutzers hinsichtlich kryptographischer Methoden nicht durch neue Gesetzgebung eingeschränkt werden sollte (Prinzip 2 der OECD-Leitlinien). Nationale Gesetzgebung, die einen gesetzmäßigen Zugriff erlaubt, soll dieses Prinzip im größtmöglichen Ausmaß reflektieren (Prinzip 6). Die Arbeitsgruppe mißt den Konsquenzen für den Datenschutz, die durch die Nutzung kryptographischer Methoden zur Sicherung der Integrität von Daten in elektronischen Transaktionen ausgelöst werden, besondere Bedeutung zu (Prinzip 5). Die Speicherung personenbezogener Daten und die Schaffung von Systemen zur persönlichen Identifikation in Verbindung mit der Nutzung solcher Methoden erfordern spezielle Maßnahmen zum Datenschutz.

(Die französischen Mitglieder der Arbeitsgruppe haben an der Verabschiedung dieser Erklärung nicht teilgenommen. Die britische Datenschutzbeauftragte hat Vorbehalte gegen diese Erklärung.)

Common Statement on Cryptography
– 12 September 1997 –

The protection of privacy and personal correspondence against arbitrary intrusions is a human right (Art. 12 Universal Declaration of Human Rights; Art. 17 International Covenant on Civil and Political Rights; Art.8 European Convention on Human Rights). In the Information Society where communication takes place mainly via telecommunications facilities this means that everybody has a right to have his electronically transmitted messages treated confidentially and that no unauthorised person can intercept their contents.

Following a proposal of the International Working Group on Telecommunications and Media the 7th International Conference of Data Protection and Privacy Commissioners has pointed out in a resolution at its session in Luxembourg on 26 September 1985, that integration and digitalisation increase the danger of unauthorised recording and evaluating of transmitted information. The 11th Inter-

national Conference of Data Protection and Privacy Commissioners at its session on 30 August 1989 in Berlin has called for data security facilities to be offered against unauthorised access, manipulation, interception and for guaranteeing the authenticity of the sender on the highest technical level and at acceptable costs.

The only measure meeting these demands is the encryption of messages. The offer of sufficient encryption methods for the users of telecommunications services is therefore essential for guaranteeing privacy. It is also a key element of privacy-enhancing technologies. With respect to mobile communications the 12th International Conference of Data Protection and Privacy Commissioners at its session on 19 September 1990 in Paris called for network operators to be obliged to offer subscribers to mobile telephone networks effective encryption procedures. The offer of end-to-end encryption facilities has been a key demand of Data Protection Commissioners when discussing the Draft European Telecommunications Directive (cf. Art. 4 of the Common Position).

The International Working Group on Data Protection in Telecommunications confirms its demand that for guaranteeing confidentiality users of electronic telecommunications services should have the opportunity to encrypt their messages on a level of their own free choice.

The prohibition of encrypting messages that is being discussed in some countries goes against this principle. It would not only hinder citizens in looking after their human right to unobservable communications, but also foster the abuse of telecommunications for illegal purposes. It could be bypassed at any time by those having the technical and financial means, so that a prohibition would only affect unsuspecting citizens.

A restriction of encryption facilities e.g. by licensing the necessary software could have the same effect. It is for the reasons mentioned above in particular not suitable to fight organised crime.

The International Working Group on Data Protection in Telecommunications understands the demands of law enforcement agencies to have access to encrypted messages for purposes of preserving public security and criminal prosecution. The 14th International Conference of Data Protection and Privacy Commissioners on 29 October 1992 in Sydney has welcomed a report by the Working Group on the access of law enforcement agencies to telecommunications contents. The Conference agreed that the technical and legal development in the field of telecommunications secrecy had to be monitored closely to protect the privacy of the individual against excessive surveillance.

The Working Group doubts that any regulation of encryption facilities for the purposes of law enforcement agencies can contribute adequately to fighting seri-

ous crimes. An intrusion on telecommunications secrecy for fighting less serious offences would be excessive anyway. All the measures that have been discussed (licensing of software, regulation of import and export, deposit of keys, hardware back-doors like the „clipper-chip“) would lead to a weaker protection, as these solutions could also be used illegally. The enforcement of legal requirements only to use certain licensed keys would reverse the relationship between confidentiality as a rule and lawful access as an exception. Since legal requirements in this field can easily be bypassed (e.g. by using hidden codes) this would amount to excessive and in the end futile surveillance of the individual.There is therefore a difference between interference with traditional forms of correspondence and with electronic communications: Interference with the former may be legal if it „… is necessary in a democratic society … for the prevention of disorder or crime …“ (Art. 8 para.2 European Convention on Human Rights); interference with the latter for the purpose of enforcing limitations of the use of cryptographic methods could lead to the abandonment of confidential electronic communications altogether.

The International Working Group on Data Protection in Telecommunications welcomes the OECD Guidelines for Cryptography Policy of 27 March 1997 as well as the Ministerial Declaration of the European Ministerial Conference (Bonn, 6-8 July 1997) which stress the importance of trustworthy cryptographic methods in order to generate user confidence in reliable information and communications systems. The OECD Guidelines also underline the principle that free user choice of cryptographic methods should not be limited by new legislation (Principle 2 of the OECD Guidelines). National policies allowing for lawful access must respect this principle to the greatest extent possible (Principle 6). The Working Group attaches particular importance to the privacy implications raised by cryptographic methods being used to ensure the integrity of data in electronic transactions (Principle 5). The collection of personal data and the creation of systems for personal identification in connection with the use of these methods require special privacy safeguards to be established.

(The French Members of the Working Group did not participate in the adoption of this Statement. The UK Data Protection Registrar has reservations vis-á-vis this statement.)

1998

23. Sitzung, 14. und 15. April 1998, Hong Kong SAR, China

Gemeinsamer Standpunkt zu Datenschutz bei Suchmaschinen im Internet

– überarbeitet und aktualisiert auf der 39. Sitzung, 6./7. April 2006, Washington, D.C. (USA) –

Gegenwärtig enthält das Internet eine riesige Menge an Informationen über fast jeden Sachverhalt, den man sich vorstellen kann. Zum Auffinden der gewünschten Information im Internet sind Suchmaschinen zu einem unverzichtbaren Werkzeug geworden. Sie sind die Schlüssel zum „cyberspace".

Mit diesen Suchmaschinen kann man nach veröffentlichten personenbezogenen Daten suchen. Als Ergebnis erhält man ein Profil der Aktivitäten einer bestimmten Person im Internet. Suchmaschinen können auch für das „data-mining" genutzt werden. Da das Internet für den Austausch von Informationen und andere Aktivitäten (z. B. den elektronischen Geschäftsverkehr) immer populärer wird, kann dies zu einer Gefährdung der Privatsphäre führen.

Darüber hinaus können Betreiber von Suchmaschinen detaillierte Profile der Interessen ihrer Nutzer erstellen. IP-Protokolldaten ermöglichen die Identifizierung von Nutzern, insbesondere dann, wenn sie mit entsprechenden bei Zugangsdiensteanbietern gespeicherten Daten kombiniert werden. Da die Nutzung von Suchmaschinen heutzutage eine gängige Praxis unter Nutzern des Internet darstellt, ermöglichen bei den Betreibern populärer Suchmaschinen gespeicherte Verkehrsdaten detaillierte Profile über Interessen, Meinungen und Aktivitäten über verschiedene Bereiche hinweg (z. B. Beruf, Freizeit, politische Meinungen, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten haben sich bereits in der Vergangenheit besonders besorgt über die Möglichkeit gezeigt, Persönlichkeitsprofile von Bürgern zu erstellen. Dies ist jetzt in einem gewissen Maß auf globaler Ebene durch die im Internet zur Verfügung gestellte Technologie möglich geworden.

Die Arbeitsgruppe hat bereits in der Vergangenheit Probleme des Datenschutzes und der Privatsphäre im Zusammenhang mit der Nutzung des Internet betont und Empfehlungen zu möglichen Schritten zur Lösung dieser Probleme gegeben. Im Hinblick auf übermittelte oder veröffentlichte personenbezogene Daten erinnert die Arbeitsgruppe daran, dass auch personenbezogene Daten, die der Nutzer freiwillig veröffentlicht hat, auch dann noch den für sie geltenden Schutzbestimmungen unterliegen.

Empfehlungen

Nutzer des Internets können gleichzeitig auch Informationsanbieter sein. Sie sollten sich darüber im klaren sein, daß jedes personenbezogene Datum, das sie im Netz publizieren (z. B. bei der Einrichtung ihrer eigenen Homepage, oder bei der Veröffentlichung von Artikeln in newsgroups), von Dritten für die Erstellung eines Profils genutzt werden kann.

So können zum Beispiel Nachrichten in newsgroups oder bei „social networking" Angeboten von Suchmaschinen durchsucht und indexiert werden, und damit zur Anreicherung von Profilen darüber beitragen, wer sich zu welchem Thema wie geäußert hat. Eine Möglichkeit, diese Gefährdung für die Privatsphäre zu reduzieren kann zum Beispiel bei der Teilnahme an newsgroups in der Nutzung von Pseudonymen bestehen.

Daher sollten Diensteanbieter und Softwarehersteller im Internet ihren Nutzern die Nutzung ihrer Dienste unter Pseudonym anbieten. Jedenfalls sollten die Nutzer auf das Risiko aufmerksam gemacht werden, das sie eingehen, wenn sie an News-Diensten, chat-Räumen oder „social networking"-Angeboten unter ihrer echten E-mail-Adresse oder sogar ihrem wirklichen Namen teilnehmen.

Die Nutzer sollten die Möglichkeit haben, die Nutzung ihrer Daten auf bestimmte Zwecke zu beschränken. Sie sollten darüber hinaus in die Lage versetzt werden, ihre eigenen Informationen im Netz (oder Teile davon) gegen die Überwachung durch Suchmaschinen zu schützen. Dies kann zum Beispiel durch das Setzen einer „no-robots"-Option für eine Website erreicht werden. Allerdings setzt die Wirksamkeit dieser Einrichtung voraus, daß sie von den Anbietern von Suchmaschinen beachtet wird.

Anbieter von Suchmaschinen sollten die Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung ihrer Dienste informieren.

Sie sollten darüber hinaus den Betroffenen ein Mittel zur Verfügung stellen, um ihre Daten aus (veralteten) möglicherweise bei den Anbietern gespeicherten Kopien von Seiten löschen zu lassen („cache").

Im Hinblick auf die Sensibilität der Spuren, die Betroffene bei der Nutzung von Suchmaschinen hinterlassen, sollten Betreiber von Suchmaschinen ihre Dienste in datenschutzfreundlicher Weise anbieten. Insbesondere sollten sie keine Informationen über Suchvorgänge, die mit einzelnen Nutzern in Verbindung gebracht werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende einer Suchmaschinen-Sitzung sollten keine Daten gespeichert bleiben, die mit einem einzelnen Nutzer in Verbindung gebracht werden können,

außer der Nutzer hat seine ausdrückliche, informierte Einwilligung zur Speicherung von zur Erbringung eines Dienstes erforderlichen Daten gegeben.

Der Minimierung von Daten kommt in jedem Fall eine Schlüsselposition zu. Eine solche Praxis wäre auch im Interesse der Anbieter von Suchmaschinen, die zunehmend mit Forderungen Dritter nach nutzerspezifischen Informationen umgehen müssen.

Zum Schutz der Privatsphäre der Benutzer ist der umfassende Einsatz von datenschutzfreundlichen Technologien erforderlich, wo dies möglich ist.

23rd meeting, 14th and 15th April 1998, Hong Kong SAR, China

Common Position on Privacy Protection and Search Engines

– revised and updated at the 39th meeting on 6–7 April 2006 in Washington D.C. –

Today, the Internet contains a vast amount of information on almost every topic one can think of. In order to be able to find the requested information on the net, search engines have become an indispensable tool. They are the keys to cyberspace.

With these search engines, it is possible to search for personal data which have been published. The result would be a profile of the network activities of a particular person. Search engines can also be used for "data mining". As the Internet is becoming more and more popular for the exchange of information and other activities (e.g. Electronic Commerce), such activities can cause a threat to privacy.

Furthermore, providers of search engines have the capability to draw up a detailed profile of the interests of their users. IP-logs, especially when combined with respective data stored with access providers, allow for the identification of users. Given that the use of search engines is nowadays common practice among netizens, traffic data stored with providers of popular search engines will allow for a detailed profile of interests, thoughts and activities across different sectors (for example work, leisure, political opinions, or even sexual preferences).

Data Protection and Privacy Commissioners have been especially concerned about the possibility to drawing up profiles of citizens in the past. Now the technology available on the Internet makes this practice, to a certain extent, technically possible on a global basis.

The Working Group has already in the past stressed the data protection and privacy problems related to the use of the Internet and has made recommendations for possible steps to solve these problems. With regard to disclosed or published personal data, the Working Group recalls that personal data which the user has voluntarily made public are still under the protection attached to their nature.

Recommendations

Users of the Internet can also be providers of information. They should be aware that every bit of personal information they publish on the net (e.g. when creating their own homepage, or publish articles in newsgroups) can be used by third parties for profiling.

For example, messages in news groups or on social networking websites can be indexed and traced by search engines, thus adding information to profiles about who expressed which opinion on which subject. One way to reduce this threat to privacy e.g. when participating in news services could be the use of pseudonyms.

Internet service providers and software manufacturers should therefore offer pseudonym services to their customers. In any case, users should be made aware of the risks they are taking when participating in news services, chatrooms or social networking sites under their real e-mail addresses or even their real names.

Users should have the option to limit the use of their data to certain purposes. They should also be capable of excluding their own personal information (or parts thereof) on the net from being monitored by search engines. This can for example be achieved by defining a “no-robots”-option for a website. However, this feature depends on being observed by the providers of search engine services.

Providers of search engines should inform users upfront in a transparent way about the processing of data in the course of using their services.

They should also provide the data subjects with a means to have their data deleted from (outdated) copies of web pages that they may store (“cache”).

In view of the sensitivity of the traces users leave when using a search engine, providers of search engines should offer their services in a privacy-friendly manner. More specifically, they shall not record any information about the search that can be linked to users or about the search engine users themselves. After the end of the search session, no data that can be linked to an individual user should be kept stored unless the user has given his explicit, informed consent to have data stored which are necessary to provide a service.

In any case, data minimization is key. Such a practice would also be beneficial for the providers of search engines who increasingly have to deal with demands for user-specific information from third parties.

To protect the privacy of the user, full application of privacy enhancing technologies is required where possible.

Gemeinsamer Standpunkt im Hinblick auf Invert-Suche in Teilnehmerverzeichnissen

Inverse Verzeichnisse werden durch Verarbeitung personenbezogener Daten aus Teilnehmerverzeichnissen erzeugt. Die Nutzung inverser Verzeichnisse zur Erlangung der Identität und der Adresse einer Person aufgrund einer Telefon- oder Telefax-Nummer oder einer E-mail-Adresse kann erhebliche negative Auswirkungen auf den Datenschutz haben und sollte daher spezifischen Regelungen zum Schutz des Persönlichkeitsrechts unterliegen.

In einigen Staaten existieren Regelungen, die den auf ihrem Territorium ansässigen Anbietern von Telekommunikation das Angebot von inversen Verzeichnissen verbieten. In diesem Zusammenhang stellen die Teilnehmer an der Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 14. und 15. April 1998 in Hong Kong fest, dass

– die Existenz inverser Verzeichnisse ohne spezielle Schutzvorschriften zur Gefährdung des Datenschutzes im Rahmen privater Beziehungen zwischen Personen führen kann;

– die kommerzielle Nutzung inverser Verzeichnisse möglicherweise schädliche Konsequenzen für Personen haben kann, die ausschließlich ihre Telefonnummer angeben wollten, insbesondere im Zusammenhang mit Kleinanzeigen in Zeitungen;

– der Zweck eines inversen Verzeichnisses nicht identisch mit dem Zweck eines Telefonverzeichnisses ist; mit einem Telefonverzeichnis ist es möglich, die Telefonnummer einer bekannten Person auf Grundlage ihres Namens und eines geographischen Kriteriums zu erhalten, während der Zweck eines inversen Verzeichnisses in der Suche nach der Identität und der Adresse von Teilnehmern besteht, bei denen nur die Telefonnummer bekannt ist;

– Teilnehmer das Recht haben müssen, nicht in Telefonverzeichnisse aufgenommen zu werden oder der kommerziellen Nutzung ihrer Daten zu widersprechen, wie dies bereits in der Gemeinsamen Erklärung der Arbeitsgruppe bei

ihrer Sitzung in Berlin im Jahre 1989 dargelegt wurde. Dass eine Person, der nur die Telefonnummer des Teilnehmers bekannt ist, dessen Adresse und Identität durch Nutzung eines inversen Verzeichnisdienstes erhält, sollte nur mit Einwilligung des Teilnehmers möglich sein;

– obwohl das Umsortieren in ein inverses Verzeichnis in manchen Fällen legitimen Interessen dienen kann, wie dem Schutz von Menschenleben oder der öffentlichen Sicherheit, die regelmäßige Bekanntgabe der Identität und der Adresse eines Teilnehmers auf der Basis seiner Telefonnummer eine unzulässige Erhebung von Informationen darstellt, wenn die Teilnehmer der Bekanntgabe ihrer Daten durch einen solchen Dienst nicht im Vorhinein widersprechen konnten;

– auch die Verarbeitung von Abrechnungsdaten, Einzelverbindungsnachweisen oder der Anzeige der Nummer des Anrufenden im Hinblick auf die Möglichkeit zur Invert-Suche oder von inversen Verzeichnissen analysiert werden muss.

Sie stimmen darin überein, dass, wo inverse Verzeichnisse nicht durch Gesetz verboten sind,

– diese Dienste eine ausdrückliche freiwillige Einwilligung erfordern. Wenigstens ein Widerspruchsrecht und das Recht auf Auskunft, die generell von existierenden nationalen und internationalen Regelungen über den Schutz personenbezogener Daten anerkannt sind, sollten garantiert werden;

– es in jedem Fall notwendig ist, den Teilnehmern bei der Datenerhebung ein Recht auf Information durch die Anbieter von Telefon- oder E-mail-Diensten über die Existenz von Diensten zur Invert-Suche einzuräumen. Falls die ausdrückliche Einwilligung nicht erforderlich ist, müssen die Teilnehmer das Recht zum Widerspruch haben und auf dieses Recht hingewiesen werden.

Common Position relating to Reverse Directories

The reverse directories are processes of personal data constituted from the directories. The process consisting in obtaining the identity and address of a person from a calling number (phone or fax) or from an e-mail can have some important negative effects on privacy and should, from them on, be subjected to specific rules of protection of the rights of persons.

However, some States have regulations forbidding the operators of telecomunications settled on their territory to offer services of reverse directories. In this context, the delegations which met in Hong-Kong on April, l4th and l5th 1998

in the International Working Group on Data Protection in Telecommunications, observe that,

– In the framework of private relations between persons, the existence of reverse directories, without specific rules of protection, can give rise to serious threats to privacy;

– The commercial utilization of reverse directories can have consequences likely to be harmful to the persons who, especially on the occasion of the diffusion of a rent or sale proposition, would have wished to indicate only their phone-number;

– The purpose of a reverse directory is not the same as the purpose of a phone directory; a phone directory allows to obtain the phone number of a known person, from his name and a geographic criterium, whereas the purpose of a reverse directory is the search of the identity and address of subscribers where only their phone number is known;

– The fact for a subscriber to appear in a phone directory must Iead, as shown by the common position expressed by the International Working Group at its meeting in Berlin in 1989, to the right not to appear in it or to oppose to the commercial utilization of his (or her) data, but he could agree that a person who would only have his phone number, may obtain his address and identity by using a service of reverse search.

– Although, the resort to a reverse directory may serve some legitimate interests in some cases, such as the protection of human life or public safety, the regular communication of the identity and address of a subscriber on the basis of his phone number, if it is carried out with regard to persons who could not beforehand have objected to the utilization of such a device with regard to them, constitutes an unfair collection of information.

– The process relating to invoicing data, detailed invoicing or to the presentation of a number of the calling line, now, shall be analyzed considering the services of reverse search or reverse directory; agree that, if the reverse directories are not forbidden by law,

– they are services which require the express consent given voluntarily. At least the right to object and the right of access generally recognized by existing national and international rules on the protection of personal data shall be guaranteed;

– It is in any case necessary to endow the persons with the right to be informed by their provider of telephone or e-mail service, at the time of the collection

of data concerning them, or if they have already subscribed, by a specific means of information, of the existence of services of reverse search and – if express consent is not required – of their right to object, free of charge, to such a search.

Gemeinsamer Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation

1. Während der Einzelne die vertrauliche Behandlung seiner privaten Kommunikation erwarten können muss, können andere öffentliche Interessen in bestimmten Fällen das Abhören durch die zuständigen Behörden rechtfertigen.

2. Das Abhören sollte nur unter besonderen Umständen erlaubt sein, wo es aufgrund schwerer Verbrechen gerechtfertigt ist, und angemessenen Schutzmaßnahmen unterliegen – wie der richterlichen Anordnung, der Benachrichtigung der Betroffenen, Beschränkungen der Nutzung und Anforderungen an die Vernichtung von Tonbändern und Protokollen. (Dieses Papier behandelt weder diese Angelegenheiten noch Fälle, in denen das Abhören möglicherweise für den technischen Betrieb von Netzen oder Zwecke der Regulierungsbehörden erforderlich ist.)

3. Das autorisierte Abhören muss notwendigerweise ohne das vorherige Wissen der Betroffenen ausgeführt werden. Allerdings sollten zur Einhaltung der Prinzipien der Offenheit, der Transparenz und der Verantwortlichkeit Mechanismen geschaffen werden, um die Öffentlichkeit zu versichern, dass die Möglichkeit zum Abhören gesetzmäßig, angemessen und verhältnismäßig genutzt wird.

4. Solche Mechanismen sollten einschließen:

   - das Führen von Protokollen
   - Überwachung und Kontrolle
   - regelmäßige öffentliche Berichterstattung.

5. *Protokollierung:* Behörden, die Abhörmaßnahmen durchführen, sollten angemessene Protokolle zum Nachweis der gesetzlichen Befugnis und der Rechtmäßigkeit jeder Abhörmaßnahme führen. Die Verpflichtung zur Führung von Protokollen könnte auch auf die beteiligten Anbieter von Telekommunikationsdiensten ausgedehnt werden.

6. *Überwachung und Kontrolle:* Einer Einrichtung, die unabhängig von der untersuchenden Behörde ist, sollte die Aufgabe zugewiesen werden, die Einhaltung der Abhörgesetze zu überprüfen; sie sollte die notwendigen Befugnisse, Möglichkeiten und Ressourcen haben, Untersuchungen durchzuführen.

7. *Offentliche Berichterstattung:* In regelmäßigen Abständen sollten Übersichten öffentlich zugänglich gemacht werden, die den Umfang und die Merkmale von Abhöraktivitäten dokumentieren, umso den gesamten Grad des Eindringens in die Privatsphäre anzuzeigen. Berichte können Statistiken enthalten über:

   - die Anzahl der angeordneten Abhörmaßnahmen und ihre Dauer
   - die Anzahl der abgelehnten Anträge auf eine Abhörmaßnahme
   - Genehmigungen mit besonderen Merkmalen oder Bedingungen (wie z. B. die Befugnis, private Grundstücke zu betreten)
   - die Anzahl der abgehörten Kommunikationsvorgänge und der identifizierten Einzelpersonen
   - die Art der verschiedenen abgehörten Kommunikationsdienste (wie Telefon, Fax, E-mail, Pager und Sprachbox-Dienste)
   - generelle Klassifizierungen von Orten, an denen Abhörmaßnahmen durchgeführt wurden (z. B. Geschäftsräume, Privatwohnungen, Fahrzeuge)
   - die Art der untersuchten Straftaten
   - die Resultate und die Effektivität von Abhörmaßnahmen, wie z. B. Fälle, in denen keine Hinweise für Verstöße gefunden wurden, in denen Anklage erhoben wurde und in denen Abhörprotokolle als Beweismittel verwendet wurden und ein Schuldspruch erreicht wurde
   - die Kosten von Abhörmaßnahmen.

Die Informationen in den Berichten sollten in klarer und verständlicher Weise gefasst sein; sie sollten Trends und besondere Eigenschaften von Abhöraktivitäten während des Berichtszeitraums enthalten.

Common Position on Public Accountability in relation to Interception of Private Communications

1. While individuals should have a reasonable expectation of being able to communicate in private, other public interests will sometimes justify interception by appropriate authorities.

2. Interception should only be permitted in exceptional circumstances where justified in serious cases and subject to appropriate safeguards – such as judicial authorisation, notification of individuals, limits on use, and requirements for destruction of tapes and transcripts. (This paper does not attempt to deal with these issues, or with interception that may be required for the technical operation of networks or for the purposes of regulatory authorities.)

3. Authorised interception must necessarily be carried out without the prior knowledge of the subjects. However, to confirm with principles of openness, transparency and accountability, there should be mechanisms to re-assure the public that interception powers are being used lawfully, appropriately and proportionally.

4. Such mechanisms should include:

- record-keeping requirements
- monitoring and auditing
- periodic public reporting.

5. *Record-keeping:* Investigating agencies undertaking interception should keep appropriate records to establish the lawful authority and justification for each interception. Record keeping obligations may also apply to the telecommunications provider involved.

6. *Monitoring and Auditing:* A body independent of the investigating agency should have the role of checking compliance with interception laws, and have the necessary powers, capabilities and resources to undertake inspections.

7. *Public reporting:* Reports should be made publicly available, at reasonable intervals, documenting the scale and characteristics of interception activity, so as to indicate the overall level of intrusion into privacy. Reports may include statistics such as those on:

- the numbers of authorised interceptions and their duration
- the numbers of applications for interception authority denied

- authorisations having special features (such as authorising entry onto private premises) or conditions
- the numbers of communications intercepted and of people identified
- different methods of interception (such as telephone, fax, e-mail, pager, voice mail)
- the general classes of places where interceptions were undertaken (such as business, private homes, cars)
- the nature of the offences under investigation
- the outcome and effectiveness of interceptions such as cases where no evidence of wrongdoing was found, prosecutions were commenced, transcripts were entered into evidence and convictions were secured
- the costs of interception.

Information in reports should be presented in a clear and meaningful manner, and should include illustration of trends and significant features of interception activity during the reporting period.

Gemeinsamer Standpunkt zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien (z. B. P3P) im WorldWideWeb

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation unterstützt jegliche Bemühungen zur Entwicklung von Technologien, die den Schutz der Privatsphäre der Benutzer im WorldWideWeb verbessern helfen.

Unter diesem Gesichtspunkt hat die Arbeitsgruppe mit besonderem Interesse auf ihrer 22. Sitzung in Berlin am 2. September 1997 und der 23. Sitzung in Hong Kong am 14. April 1998 von dem Platform for Privacy Preferences Project (P3P) Kenntnis genommen, das gegenwärtig durch das WorldWideWeb-Konsortium durchgeführt wird.

Obwohl noch eine Reihe von technischen Details zu klären ist, einschließlich des Ausmaßes, in dem Punkte wie Datensicherheit, Qualität der Daten, Speicherungsdauer sowie Auskunft und Berichtigung von Daten behandelt werden sollen, möchte die Arbeitsgruppe die folgenden grundlegenden Bedingungen darlegen, die von jeder technischen Plattform für den Datenschutz im WorldWideWeb mit dem Ziel der Verhinderung einer systematischen Sammlung personenbezogener Daten berücksichtigt werden sollten:

1. Technologie allein kann nicht die Lösung zur Sicherstellung des Datenschutzes im Web sein. Sie muss innerhalb eines regulatorischen Rahmens angewandt werden (dieser kann sowohl in gesetzlichen Regelungen als auch in Verträgen und Verhaltensregeln bestehen, die gleichartige Garantien im Hinblick auf ihre Durchsetzung bieten, einschließlich Sanktionen, eines effektiven und unabhängigen Überwachungssystems und Rechtsschutzes für den Einzelnen).

2. Jeder Nutzer sollte die Möglichkeit haben, das Web anonym zu benutzen. Das betrifft auch das Herunterladen öffentlich zugänglicher Informationen. Personenbezogene Informationen sollten in diesem Fall nur für den Zeitraum verarbeitet werden, in dem der Nutzer die Website liest, mit Ausnahme der Verbindungsdaten, soweit diese für Sicherheitszwecke erforderlich sind.

3. Bevor personenbezogene Daten, insbesondere solche, die durch den Benutzer offenbart wurden, durch den Anbieter einer Website verarbeitet werden, ist eine informierte Einwilligung des Benutzers erforderlich. Darüber hinaus sollten einige unabdingbare Grundregeln in die Standardkonfiguration der technischen Plattform eingebaut werden. Personenbezogene Daten dürfen nicht in einem automatischen Verfahren zu einer Website ohne vorherige Information des Betroffenen übertragen werden, der stets die Möglichkeit haben sollte, die Übertragung zu verhindern.

4. Die Implementierung des P3P-Projekts wird von entscheidender Bedeutung sein und sollte genau beobachtet werden.

Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the WorldWideWeb

The International Working Group on Data Protection in Telecommunications supports any effort to develop technologies which help to improve the protection of user privacy in the WorldWideWeb.

In this respect the Working Group has with particular interest at its 22nd meeting in Berlin on 2 September 1997 and at its 23rd meeting in Hong Kong on 14 April 1998 taken note of the Platform for Privacy Preferences Project (P3P) which is currently promoted by the WorldWideWeb Consortium.

While a number of technical details still need to be clarified, including the extent to which issues such as security, data quality, periods of retention and access and correction are dealt with, the Working Group wishes to set out the following essential conditions that should be met by any technical platform for privacy protec-

tion on the WorldWideWeb with the objective of avoiding a systematic collection of personal data:

1. Technology cannot in itself be the solution for securing privacy on the Web. It needs to be applied according to a regulatory framework (enshrined in law as well as contracts and codes of conduct providing similar guarantees in terms of their enforcement, including sanctions and an effective and independent auditing system and legal recourse for the individual).

2. Any user should have the option to browse the Web anonymously. This applies also to the downloading of information in the public domain. Personal information should in this case only be processed as long as the user is reading the website, except for the connection data so far as necessary for the purpose of security.

3. Before personal data, in particular those disclosed by the user, are processed by the provider of a website, the user's informed consent is necessary. Moreover, certain non-waivable groundrules should be built into the default configuration of the technical platform. Personal data must not be transmitted to a website in an automatic procedure, without prior notification to the data subject who should always have the option to block the transmission.

4. The implementation of the P3P-Project will be of crucial importance and needs to be closely monitored.

1999

25. Sitzung, 29. April 1999, Norwegen

Gemeinsamer Standpunkt zu Datenschutz bei Gebäude-Bilddatenbanken

Computer haben die Fähigkeit, Informationen aus einer Reihe von Quellen einschließlich öffentlicher Register zu verknüpfen und zugänglich zu machen. Im Zusammenhang mit der Entwicklung von Geographischen Informationssystemen (GIS), die die Ortsbestimmung ermöglichen, und digitaler Fotografie- bzw. Bilderstellung kann dies das leichte Auffinden großer Informationsmengen durch Verknüpfung mit Adressen oder Planangaben (-koordinaten) ermöglichen. Darin liegt eine wachsende Bedrohung für die Privatsphäre einzelner Bürger. Eine aktuelle

Entwicklung ist die systematische Sammlung digitaler Bilder von Gebäuden zum Aufbau von Gebäude-Bilddatenbanken ganzer Städte für kommerzielle Zwecke. Während es wichtige und legitime Anwendungen für Geographische Informationssysteme und digitale Aufnahmen von Gebäuden gibt, z. B. für Planungszwecke, muss die Position der Betroffenen hinsichtlich der kommerziellen Nutzung dieser Datenbanken gestärkt werden.

So setzen gegenwärtig beispielsweise Unternehmen in mehreren Ländern mobile Digitalkameras ein, die auf Kleintransportern montiert sind, um Bilder aller Gebäude in größeren Städten aufzuzeichnen. Die Daten können dann auf CD-ROM gespeichert und der Feuerwehr, der Polizei und Notfalldiensten zur Vorbereitung ihrer Einsätze angeboten werden. Es liegt aber auf der Hand, dass eine solche Datenbank auch für kommerzielle Zwecke genutzt werden kann. Die Bilder können mit Hausnummern, Namen und Adressen von Eigentümern und Bewohnern zur Beurteilung der Bonität (Scoring) oder Risiken durch Banken und Versicherungen auf Grund des Gebäudezustandes oder einer Einstufung der Wohngegend bzw. für Zwecke der Direktwerbung verknüpft werden. Die Daten können für fernsehgestützte Bilddatenbanken oder für Planungszwecke von Transportunternehmen (Lieferfirmen,Taxis usw.) verwendet werden. Sie werden oft mit Daten verknüpft, die mit Hilfe von Satelliten erhoben werden (Global Positioning System – GPS), und können dann genutzt werden, um realistische digitale Stadtpläne zu erzeugen und eine neue Generation Geographischer Informationssysteme zu unterstützen. Obwohl gegenwärtig – abhängig vom eingesetzten System – Probleme der Speicherkapazität und Verarbeitungsgeschwindigkeit auftreten können, wird sich dies wahrscheinlich ändern.

Es muss deutlich gemacht werden, dass eine totale Registrierung aller Gebäude in einer Stadt oder in einem Land zu einer Verarbeitung personenbezogener Daten führen wird, da ein Großteil der Informationen sich auf natürliche Personen bezieht, die durch Zuordnung zu spezifischen Elementen als Ausdruck ihrer physischen, wirtschaftlichen, kulturellen oder sozialen Identität bestimmbar sind (vgl. Artikel 2 a) und c) der Richtlinie 95/46/EG) und die direkt oder indirekt mit Verzeichnissen verknüpft werden können. Deshalb unterliegt die Schaffung von Bilddatenbanken dieser Art den nationalen Datenschutzgesetzen in Übereinstimmung mit der EG-Datenschutzrichtlinie. Wo dies nicht bereits der Fall ist, sollte die nationale Gesetzgebung dem Betroffenen zumindest ein Widerspruchsrecht gegen die systematische Sammlung und Speicherung derartiger Bilddaten über seine Wohnumgebung für kommerzielle Zwecke einräumen. Die Tatsache, dass diese Informationen bereits zu einem gewissen Grad öffentlich zugänglich sind, schließt sie nicht von der Anwendung der Datenschutzgesetze aus. Darüber hinaus kann die Veröffentlichung solcher Datenbanken Sicherheitsprobleme für die Betroffenen (Eigentümer, Mieter oder Bewohner) verursachen. Es gibt einen Unterschied zwischen einem einzelnen Bürger, der für private Zwecke Aufnahmen eines bestimmten Gebäudes macht, und einem Unternehmen, das systematisch

Bilder aller Gebäude in einer Stadt für kommerzielle Zwecke sammelt. Insbesondere muss der Betroffene das Recht haben, einer Einstellung dieser Daten in das Internet oder ihrer Speicherung auf elektronischen Datenträgern (z. B. CD-ROM) jederzeit zu widersprechen.

25th meeting, 29th April 1999, Norway

Common Position on Data Protection Databases of Images of Buildings

Computers have the capacity to bring together, and facilitate easy access to, information from a range of sources including public registers. When taken with such developments as Geographical Information Systems, which allow referencing by location, and digital imaging, this can allow the easy retrieval of a great deal of information by reference to an address or map reference. This presents a growing threat to the privacy of private citizens. A recent development is the systematic collection of digital images of dwellings to create building databases of cities for commercial purposes. While there are important and legitimate applications for Geographical Information Systems (GIS), and digital images of buildings, e.g. for planning purposes the position of data subjects with regard to the commercial use of these databases need to be strengthened.

For example in several countries companies are currently using mobile digital cameras mounted on minivans to collect images of all buildings in major cities. The data may be pressed on CD-ROMs and may be offered to fire brigades, police, and emergency services to enable them to prepare for their operations. It is however self-evident that such a database may be used for commercial purposes as well. The images may be linked to house numbers, names, and addresses of owners or inhabitants for scoring and risk assessment purposes (condition of the building, ranking of neighbourhoods) by banks and insurances and for direct marketing. The data could be used by TV or for planning purposes of carriers (delivery firms, taxis, etc.). They are often linked to data collected by satellite (Global Positioning System – GPS -) and they can be used to generate realistic digital city maps and to form a new generation of Geographical Information Systems. Although at present depending on the system used there may be problems of storage capacity and speed which prevent these data being put on the Internet at reasonable costs, that is likely to change.

It should be made clear that a total scan of all buildings in a city or a country will involve the processing of personal data since much of the information relates to natural persons who are identifiable by factors specific to their physical, economic, cultural, and social identity in a data filing system (Art. 2 a) and c) of Directive

95/46/EC) and may be linked directly or indirectly to directories. Therefore the creation of image data bases of this kind falls within the scope of national data protection laws in accordance with the EC Data Protection Directive. Where this is not the case already, national legislation should at least provide the data subject with a right to object against the systematic collection and storage of such image data referring to his dwelling for commercial purposes. The fact that this information is to some extent already in the public domain does not exclude it from the application of data protection laws. In addition the publication of such databases may cause security problems to the data subjects (i.e. owners, tenants or inhabitants). There is a difference between an individual taking pictures of a specific building for personal reasons and a company systematically collecting images of all buildings in a city for commercial purposes. In particular the data subject must have the right to object at any given time to these data to be put on the Internet or other electronic media (e.g. CD-ROM).

Gemeinsamer Standpunkt zu intelligenten Software-Agenten

Ein Software-Agent wird definiert als ein Software-Produkt, das anstelle seines Benutzers agiert und versucht, ohne einen direkten Eingriff oder eine direkte Überwachung des Benutzers bestimmte Objekte zu finden oder bestimmte Aufgaben zu erledigen. Agenten können in verschiedener Weise bei der Telekommunikation verwendet werden. An erster Stelle können sie dazu benutzt werden, die Funktionalität eines Telekommunikationsnetzes zu erweitern. Es ist möglich, ein Netzwerk effizienter zu benutzen, wenn die Ressourcen an die Anforderungen der einzelnen Nutzer angepasst sind. Agenten können diese Aufgabe übernehmen, in dem sie die Nutzer repräsentieren.

Eine andere Anwendung bezieht sich auf inhaltliche Mehrwertdienste, die mit Mitteln der Telekommunikation verbreitet werden: Agenten können im Auftrag des Nutzers verwendet werden, um Informationen (z. B. im Internet) zu selektieren und zu sammeln, sowie als Mittler gegenüber anderen Teilnehmern bei elektronischen Transaktionen auftreten. Im Augenblick stehen die ersten Dienste dieser Art zur Verfügung, ausgehend von einer einfachen „Push-Technologie", die Informationen auf der Basis individuell spezifizierter Interessen dem Benutzer ins Haus bringt, bis hin zu komplizierten Systemen, die es gestatten, die Nutzung des Netzes zu personalisieren und die Aktivitäten der Nutzer nachzuvollziehen.

Die Entwicklung der Agenten-Technologie wird in intelligenten Software-Agenten gipfeln, Software-Programmen, mitunter mit dedizierter Hardware gekoppelt, die dazu bestimmt ist, komplette Aufgaben im Auftrag der Nutzer zu erledigen. In

ihrer Rolle als Repräsentant einer Person wird eine Vielzahl personenbezogener Informationen erzeugt und durch die Operationen der Agenten verbreitet werden. Der Schutz der Privatsphäre und die Vertraulichkeit der Netzaktivitäten werden eines der größten Probleme sein, mit denen die Nutzung intelligenter Agenten in der Zukunft konfrontiert sein wird.

Dieser gemeinsame Standpunkt zielt darauf ab, eine erhöhte Aufmerksamkeit für die Risiken für die Privatsphäre zu erzeugen, die mit der Nutzung von Agenten verbunden sind, und die Systemdesigner zu ermutigen, Maßnahmen zum Schutz der Privatsphäre einzubauen. Die Risiken für die Persönlichkeitsrechte, die mit der Nutzung von Agenten verbunden sind, können wie folgt zusammengefasst werden:

1. Erstens: Risiken, die mit der Tatsache zusammenhängen, dass ein Agent im Auftrag eines Nutzers handelt. Nutzerprofile stellen einen wesentlichen Anteil der Aktivitäten von Agenten dar. Typischerweise umfasst das Nutzerprofil Informationen über Identität und Kommunikationspartner sowie eine Vielzahl von Informationen über persönliche Präferenzen. Wenn ein Agent im Netz operiert, werden personenbezogene Daten mit der Umgebung ausgetauscht und möglicherweise an nicht autorisierte dritte Parteien weitergegeben.

2. Zweitens: Risiken, die mit fremden Agenten verbunden sind, die im Auftrag anderer Teilnehmer handeln. Agenten oder allgemeiner ihre Nutzer, könnten mit Agenten konfrontiert werden, die im Auftrag anderer Teilnehmer handeln. Diese könnten freiwillig personenbezogene Daten von Individuen sammeln, indem sie eine Verkehrsanalyse durchführen, in Datenbanken eindringen, die Informationen über die Individuen enthalten, oder das Nutzerprofil eines Agenten zugänglich machen. Derartige Agenten können sogar verkleidet auftreten oder andere Agenten ausschalten.

Empfehlungen:

Maßnahmen müssen ergriffen werden, um das Auftreten von Risiken für die Privatsphäre durch intelligenten Software-Agenten zu reduzieren. Die Arbeitsgruppe empfiehlt, dass Folgendes Berücksichtigung findet, wobei die Anforderungen, die die Datenschutzprinzipien stellen, insbesondere diejenigen, die sich aus dem Zweck ergeben, für den der Agent erstellt worden ist, berücksichtigt werden müssen:

1. Software-Hersteller sollten in einem frühen Designstadium die Auswirkungen der Nutzung intelligenter Agenten für die Privatsphäre des Einzelnen bedenken. Dies ist notwendig, um die Konsequenzen, die in naher Zukunft entstehen könnten, unter Kontrolle zu halten.

2. Entwickler von Agenten sollten sicherstellen, dass die Nutzer die Kontrolle über ihre Systeme und die darin enthaltenen Informationen nicht verlieren. Sie sollten dem Nutzer ein Maximum an Transparenz über die Funktionsweise des Agenten verschaffen. Wenn Kontroll- und Feedbackmechanismen sowie Sicherheitsvorkehrungen hinzukommen, wird dies den Nutzern von Agenten helfen, Vertrauen bei der Nutzung der Agententechnologie zu verbessern.

3. Entwickler von intelligenten Agenten sollten geeignete Mittel zur Verfügung stellen, durch die die Privatsphäre der Nutzer geschützt und die Kontrolle der Betroffenen über die Nutzung ihrer personenbezogenen Daten aufrechterhalten werden kann.

4. Technische Maßnahmen sowie Privacy Enhancing Technologies (PET) werden in Verbindung mit den Software-Agenten empfohlen. Die folgenden Maßnahmen werden vorgeschlagen:

   - Entwicklung einer Trusted-Third-Party-Struktur für die Verifizierung und Authentifizierung aller Agenten
   - Zugangskontrollmechanismen
   - Werkzeuge, die dem Nutzer die Kontrolle über die Aktionen von Agenten Dritter Teilnehmer verschaffen, die personenbezogene Daten sammeln
   - Mechanismen, die aufgezeichneten Aktivitäten nachzuvollziehen
   - Integritätsmechanismen, um die Integrität der gespeicherten oder ausgetauschten Daten sicherzustellen und die Integrität der Arbeitsmethoden der Agenten oder der zertifizierten Komponenten wie digitale Signaturen zu kontrollieren.

Diese Maßnahmen müssen in die Agenten integriert werden. Die Maßnahmen können auch genutzt werden, um eine Infrastruktur vertrauenswürdiger Komponenten aufzubauen.

5. Anhand einer Checkliste für datenschutzfreundliche Designkriterien sollten die Entwickler, Lieferanten oder Provider eines Agenten den Agenten oder die Umgebung des Agenten mit geeigneten Privacy Enhancing Technologies ausrüsten. Rahmenbedingungen für die Zertifizierung der Datenschutzfreundlichkeit von Software-Agenten sind notwendig.

Common Position on Intelligent Software Agents

A software agent is defined as a piece of software that acts on behalf of its user and tries to meet certain objectives or to complete tasks without any direct input or direct supervision from its user. Agents may find several applications in telecommunications. In the first place they can be used to increase the functionality of a telecommunications network. It is possible to use a network more efficiently if the network resources are adapted to the demands of individual users. Agents can fulfil this task by representing the users.

Another application is in value-added content services that are delivered by means of telecommunications networks: agents can be applied on behalf of the user to select and gather information (e.g. on the Internet) and to act as intermediate with other parties in electronic transactions. Currently the first services of this kind start to become available, ranging from simple 'push technology' which brings information to the user's doorstep based on individually specified interests, to sophisticated systems that allow for the personalization of network user sessions and the tracking of user activities.

The development of agent technologies will culminate in Intelligent Software Agents, software programs, at times coupled with dedicated hardware, designed to complete tasks on behalf of their user. Given their role as representative of a person, a wealth of personal information will be generated and exchanged by the operations of agents. Privacy and confidentiality of actions will be amongst the major issues confronting the use of intelligent agents in the future.

This Common Position aims at increasing awareness of the privacy risks associated with the use of agents and encouraging system designers to incorporate measures to protect privacy. The privacy risks associated with the use of agents can be grouped as follows:

1. Firstly, risks associated with the fact that an agent acts on behalf of a user. User profiling is at the core of agents' activities. Typically the user profile will contain identity and contact information, as well as a great deal of information about personal preferences. When an agent operates on a network personal data will be exchanged with the environment, and potentially disseminated to unauthorised third parties.

2. Secondly, risks associated with foreign agents that act on behalf of others. Agents, or generally their users, might be confronted with agents acting on behalf of others, These might deliberately collect personal data of individuals by performing traffic flow analysis, entering databases that contain information about the individual or entering the user-profile of an individual's agent. Such agents may even appear in disguise or overrule other agents.

Recommendations

Measures have to be taken to reduce the impact of the privacy risks of Intelligent Software agents. The Working Group recommends that the following be considered, notwithstanding requirements that are necessary to comply with any data protection principles, especially those that might follow from the purpose for which the agent is constructed:

1. Producers of software agents should reflect in an early stage of design on the implications of the use of intelligent agents for the privacy of individuals. This is necessary to control the consequences that may arise in the near future.

2. Developers of agents should ensure that users do not loose control over their systems and information contained therein. They should provide the user with the maximum of transparency on the functioning of the agent. Adding control and feedback mechanisms and safeguards to prevent this will help agent-users to increase trust in using agent technologies.

3. Developers of intelligent agents should ensure the proper means by which the privacy of users may be protected and control maintained by data subjects over the uses of their personal data.

4. Technical facilities such as Privacy Enhancing Technologies (PET) are recommended in conjunction with software agents. The following measures are proposed:

   - development of a Trusted Third Party structure for the identification and authentication of all agents;
   - access control mechanisms;
   - tools to give a user control over the actions of third parties‘ agents that collect personal data;
   - mechanisms to audit the logged activities;
   - integrity mechanisms to control the integrity of stored or exchanged data and to control the integrity of working methods of agents or trusted components, like digital signatures;

These measures can be integrated into the agents. The measures can also be used to build an infrastructure of trusted components.

5. By using a checklist of privacy-compliant design criteria, the designer, supplier, or provider of an agent should design or equip an agent or an agent-environment with proper privacy-enhancing technologies. A framework for certification of the privacy-compliance of software agents is required.

Gemeinsamer Standpunkt zur Sprechererkennung und Stimmerkennungstechnologien in der Telekommunikation

Unter den gegenwärtig entwickelten biometrischen Identifikationsmethoden ist die Sprechererkennung wahrscheinlich die fortschrittlichste und von besonderer Relevanz für die Telekommunikation.

Sprechererkennung ist eine Methode, die Eigenschaften der Stimme einer Person zu analysieren, um

– die Stimme eines unbekannten Sprechers zu identifizieren;

– zu verifizieren, dass ein Sprecher derjenige ist, der er behauptet zu sein (Authentifikation);

– die Stimme einer Person in einer Umgebung mit vielen Sprechern zu erkennen.

In allen Fällen wird die Stimme einer Person gemessen und mit einem zuvor aufgenommenen und gespeicherten Muster oder Stimmabdruck der Stimme verglichen.

Die besten Ergebnisse beim Erkennen der Personen werden in Bezug auf die Fehlerraten erzielt, wenn die gleichen Wörter für die Eingabe und das Muster verwendet werden (text dependent systems). Zu denken ist an ein vorher festgelegtes Passwort oder eine Identifikationsnummer. Nach der Eingabe wird dieses mit dem gespeicherten Stimmabdruck verglichen.

In anderen Systemen werden die Sprecher veranlasst, zufällig ausgewählte Wörter zu wiederholen, die mit dem Muster verglichen werden (text prompted systems). Der Vorteil ist hier, dass das System nicht fehlgeleitet werden kann durch Fälscher, die auf Band gespeicherte Stimmabdrücke missbrauchen.

In „text independent systems“ wird eine Person gebeten zu sprechen, und ihre Äußerungen werden mit den gespeicherten Mustern verglichen, die völlig verschiedene Wörter enthalten. Dies beinhaltet einen erheblich höheren Zufallsfaktor, und von daher ist der Vergleich schwieriger, besonders wenn Hintergrundgeräusche

vorliegen oder Telefonleitungen mit hohem Geräuschpegel verwendet werden. Auf der anderen Seite ist das Potential hoch: In Verbindung mit einer großen Sammlung von Stimmmustern ermöglichen textunabhängige Systeme die Identifizierung vieler verschiedener Personen in verschiedenen Umgebungen.

Die Sprechererkennung kann genutzt werden für die Identifikation und Authentifikation sowohl für den Zugang zu Netzen und Anlagen als auch für den Zugang zu Diensten, die über das Netz verbreitet werden. Offensichtlich haben Telekombetreiber ein Interesse an verbesserter Stimmidentifizierung und Authentifizierung zu verschiedenen Zwecken, z. B. Abrechnungsbetrug zu bekämpfen oder neue Funktionen und Dienste zu vermarkten. Was Dienste betrifft, die über Telekommunikationsdienste verbreitet werden, wird die Identifikation von Kunden zunehmend als wesentlich für Online-Entscheidungen betrachtet, bei denen ein Individuum beteiligt ist. Es muss bemerkt werden, dass anders als die meisten anderen biometrischen Identifikationsmethoden die Sprechererkennung keine neue Infrastruktur erfordert, sie kann vielmehr in die bestehenden Telekommunikationsnetze integriert werden.

Die Nutzung der Sprechererkennung ist noch beschränkt auf bestimmte Anwendungen. Die Kosten dieser Technologie werden erwartungsgemäß allerdings schnell sinken, während die Qualität der Systeme wächst. In naher Zukunft können Massenanwendungen erwartet werden.

Die Datenschutzbeauftragten haben bei anderer Gelegenheit festgestellt, dass anonyme Methoden für den Zugang zu Telekommunikationsnetzen und anonyme Zahlungsmethoden zwei wesentliche Elemente echter Online-Anonymität sind.

Die Internationale Arbeitsgruppe ist besorgt über das Risiko, dass diese Techniken in der Telekommunikation eingesetzt und genutzt werden können, ohne Kenntnis der Nutzer und ohne Mittel, sie zu umgehen.

Empfehlungen

1. Die Einführung und Nutzung von Sprechererkennungstechnologien in Telekommunikationsnetzen sollte auf Umstände beschränkt werden, bei denen die Authentifikation wesentlich ist.

2. Da diese Identifikationsmethode unvermeidlich eine bestimmte Fehlerquote hat, sollte sie nicht eingeführt werden, ohne dass Schadensersatzansprüche zur Verfügung stehen.

3. Die informierte Einwilligung der Betroffenen sollte eingeholt werden, bevor Sprachanalysetechnologien angewandt werden. Grundsätzlich sollte diese

Technologie auch mit deren Einwilligung nicht angewandt werden, um den geistigen oder emotionalen Zustand einer Person zu ermitteln.

4. Den Betroffenen sollte die Möglichkeit gegeben werden, anonym zu bleiben, wo dies angemessen ist.

5. Provider sollten die Betroffenen informieren, wenn ihre Stimmmuster in einer Datenbank gespeichert werden. Diese Information sollte auch klarstellen, unter welchen Umständen die Daten genutzt werden sollen.

6. Anbieter, in deren Auftrag eine Identifikation anhand einer Sprechererkennung stattfindet, sollten den Betroffenen über ihre Identität und den Zweck informieren, für den die Identifikation erforderlich ist.

Common Position on Speaker Recognition and Voice Analysis Technology in Telecommunications

Among the currently developed biometrical identification methods, speaker recognition is probably the most advanced and of particular relevance to telecommunications.

Speaker recognition is a method to analyse features of a person's voice to:

– identify the voice of an unknown speaker;

– verify that a speaker is who he or she claims to be (authentication);

– recognise a voice of a person in an environment with many speakers.

In all cases a person's voice is measured and compared to a previously recorded and stored digital template or voiceprint of his/her voice.

Best results in recognising persons, in terms of failure rates, are obtained if the same words are used for input and for the template (text dependent systems). Think of a predetermined password or ID. When entered, this is matched to a stored voiceprint.

In other systems speakers are prompted to repeat randomly selected words, which are being matched to the template (text prompted systems). An advantage is that the system cannot be misled by impostors who use voice samples recorded on tape.

Finally, in text independent systems a person is asked to talk and his utterances are matched with the stored templates, containing completely different words. This situation offers much more contingency, and hence the matching is more difficult, in particular if background noise is present or noisy telephone lines are used. On the other hand the potential of these systems is high: combined with a large database of voice templates, a text independent systems enables identification of many different persons in many circumstances.

Speaker recognition can be used for identification and authentication for both access to the network and equipment and access to the services delivered over the network. Obviously telecom operators perceive an interest in improved voice identification and authentication for various purposes, for instance fighting telecommunications fraud or marketing of new features and services. As for services delivered by means of the telecommunication networks, identification of customers is increasingly seen as an important for making on-line decisions on the way an individual is treated.

It should be noted that, unlike most other biometrical identification methods, speaker recognition does not need a new infrastructure, but can be integrated in the existing telecommunications networks.

The use of speaker recognition is still restricted to dedicated applications. The cost level of this technology is, however, expected to decline rapidly, while the quality of the systems is continuously improving. Mass applications can be expected in the near future.

Data Protection and Privacy Commissioners have stated on other occasions that anonymous means to access telecommunication networks and anonymous means of payment are two essential elements for true online anonymity.

The International Working Group is especially concerned about the risk that these techniques may be installed and used in telecommunication networks without any knowledge of the users or any means to avoid this phenomenon.

Recommendations

1. The introduction and use of speaker recognition technologies in telecommunication networks should be limited to circumstances where authentication is essential.

2. Since this identification method inevitably has a certain margin of error speaker recognition should not be introduced without offering any means to redress.

3. The informed consent of persons should be obtained before voice analysis technology is applied. In principle this technology should not be applied to derive a person‘s mental or emotional state even with that person‘s consent.

4. Persons should be given the choice to remain anonymous where appropriate.

5. Providers should inform persons if their voice templates are stored in any database. This information should also make clear in what circumstances these data will be used.

6. Parties on whose behalf identification by speaker recognition is taking place, should inform the person on their own identity and the purpose for which identification is necessary.

2000

27. Sitzung, 4. und 5. Mai 2000, Rethymnon, Griechenland

Gemeinsamer Standpunkt zur Missbrauchserkennung in der Telekommunikation

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation weist auf Probleme des Datenschutzes im Zusammenhang mit der Erkennung von Missbrauch in der Telekommunikation hin, insbesondere im Hinblick auf die Verarbeitung von Verbindungsdaten durch die Anbieter von Telekommunikationsdiensten.

Der Begriff Missbrauch wird hier im Sinne von „betrügerischer Inanspruchnahme von Telekommunikationsdiensten“ gebraucht, statt im Sinne von missbräuchlichen Aktivitäten unter Nutzung von Telekommunikationsnetzen (hacking etc.)“. Die Arten des Missbrauchs, die hier behandelt werden, schädigen die Anbieter von Telekommunikationsdiensten, weil diese Dienste anbieten, die nicht oder nur teilweise bezahlt werden, was zu einem Gewinnverlust führt.

Der Umfang des Missbrauchsphänomens in Hinsicht auf finanzielle Verluste der Anbieter ist schwer abzuschätzen. Weltweit werden Zahlen zwischen drei und sechs Prozent genannt. Es ist offensichtlich, dass ein Ansteigen des Missbrauchs zur Besorgnis bei vielen Anbietern führt, besonders weil die Margen für Telekommunikationsdienste in den liberalisierten Märkten schrumpfen. Das liegt im ureigenen Interesse der Anbieter von Telekommunikationsdiensten, diese Arten des Missbrauchs zu begrenzen.

Allgemeine Arten des Missbrauchs

Zwei allgemeine Arten des Missbrauchs sind:

Weiterverkaufs-/Gebührenbetrug. Der Weiterverkauf von Verbindungen an Dritte, ohne den Anbieter für die Verbindungen zu bezahlen. Verschiedene Konstruktionen sind möglich, oft unter Nutzung von „Telefon-Läden" („phone houses"), Durchwahl-Konstruktionen oder mobilen Endgeräten.

Mehrwertdienstebetrug. Dieser umfasst verschiedene Typen des Missbrauchs kostenintensiver, spezieller Anschlüsse (typischerweise 09-Nummern). In einigen Fällen wird der Anschluss in der Art genutzt, dass Anrufe über manipulierte Telefone zu einem Mehrwertdiensteanschluss getätigt werden. Ein weiterer Ansatz besteht darin, unter Zuhilfenahme von Mittätern Verbindungen zu solchen Mehrwertdiensten aufzubauen, z. B. nach Geschäftsschluss in Büros. Eine weitere Möglichkeit besteht darin, Nutzer, ohne dass diese sich darüber klar sind, zum Anruf bei kostenintensiven Anschlüssen zu verführen. Der Betrüger streicht dabei den Gewinn aus diesen Aktivitäten ein.

Methoden des Betrugs

Die hauptsächlichen Methoden zum Begehen eines Betrugs sind:

Betrug durch den Teilnehmer. Ein Anschluss wird durch den normalen Anmeldeprozess unter einer falschen oder gestohlenen Identität erlangt. Es ist auch möglich, dass Angestellte von Telekommunikationsdiensteanbietern bei dieser Art des Betrugs mitwirken, z. B. indem sie absichtlich Prozeduren außer Acht lassen, die zur Feststellung der Identität eines neuen Kunden dienen.

„Surfing". Diese Methode schließt verschiedene Formen der unautorisierten Nutzung von Einrichtungen ein:

Duplizierung von Endeinrichtungen. Identitäten, Telefone oder andere Attribute werden dupliziert.

Betrug mit „Calling-Cards". Dies schließt den Diebstahl oder den Betrug mit PIN-Codes und wiederaufladbaren Karten ein.

Missbrauch von Hardware. Dies schließt verschiedene Möglichkeiten zum Eindringen in Telekommunikationsnetzwerke ein.

Wenn dieses „Hacking" einmal erfolgreich war, wird das Netzwerk benutzt, ohne dafür zu zahlen. Zugang zu dem Netzwerk kann erlangt werden durch Service-

Einrichtungen in Vermittlungsstellen oder Nebenstellenanlagen, Einwahlnummern, Voice-Mail-Systeme etc.

Das Anzapfen eines anderen Anschlusses durch physikalische Verbindungen mit diesem Anschluss.

Betrug in der Mobilkommunikation. Die Mobilkommunikation eröffnet verschiedene neue Möglichkeiten zum Betrug. Spezifische Typen des Betrugs, die unter Nutzung von Mobiltelefonen begangen werden, sind die folgenden: Die einfachste Form besteht in dem einfachen Diebstahl von Mobiltelefonen. „Roaming"-Betrug ist eine andere Form; kostenintensive Gespräche werden vom Ausland aus geführt, unter Nutzung der Verzögerung, die bei der Abrechnung solcher Gespräche in dem Land entsteht, wo das Telefon registriert ist. Es wird auch über das Wiederaufladen oder Kopieren vorausbezahlter Karten berichtet. Darüber hinaus existieren auch verschiedene Arten des Betrugs im Zusammenhang mit Anrufweiterschaltung.

Betrugserkennung: Methoden

Die Bekämpfung von Betrug impliziert dessen Entdeckung. In diesem Abschnitt werden einige Hinweise gegeben, wie die Erkennung von Betrug funktioniert und welche Daten als Basis für die angewendeten Techniken genutzt werden.

Der größte Teil der für die Betrugserkennung genutzten Daten sind entweder Einzelverbindungsdatensätze (Call Detail Record – CDRs) oder Abrechnungsdaten. CDRs bestehen aus einer Sammlung von Daten, die durch das Signalisierungssystem durch das Netzwerk übertragen werden. Diese Verbindungsdaten enthalten die anrufende und die angerufene Nummer, die Zeit, die Dauer und andere für die Kommunikation notwendige Daten. In dem Abrechnungssystem werden die CDRs ausgewertet und die Rechnungen für die einzelnen Kunden erzeugt.

Systeme zur Missbrauchserkennung können grob wie folgt zusammengefasst werden:

– Analyse von auf Verbindungsdaten (CDRs) und Abrechnungsdaten basierenden Auswertungen. Dies bedeutet die Analyse der Auswertung und die Suche nach Auffälligkeiten.

– Automatisierte Werkzeuge zur Analyse von CDRs, die auf einem festen voreingestellten Regelsystem basieren. Dies kann während der Kommunikationsvorgänge oder nach deren Abschluss erfolgen. Diese Methode ermöglicht mehr Flexibilität als die einfache Analyse, mit der Möglichkeit, die entsprechenden Regeln anzupassen. Diese Systeme sind typischerweise „Expertensysteme".

– Komplexe automatisierte Systeme mit einer gewissen Lernfähigkeit und der Fähigkeit, selbst neue Regeln zur Erkennung zu entwickeln. Die hierbei gebräuchlichen Techniken sind neuronale Netze, genetische Algorithmen und Data-Warehouse-/Data-Mining-Techniken.

Zur Missbrauchserkennung genutzte Daten

Verschiedene Datenarten werden für die Missbrauchserkennung genutzt. Eine unvollständige Zusammenfassung der in diesem Prozess genutzten Daten schließt ein:

– hohe Nutzungsfrequenz,

– ansteigende Nutzungsfrequenz,

– verdächtige Nutzung, wie der plötzliche Anstieg der Nutzung von Mehrwertdiensten,

– langdauernde Verbindung, z. B. länger als acht Stunden,

– verdächtige Verbindungsziele im Ausland, die als anfällig für Betrug bekannt sind,

– Nutzung kostenintensiver Angebote, die als anfällig für Missbrauch bekannt sind,

– Nutzerprofile, die im Allgemeinen in verschiedene Risikoklassen aufgeteilt sind,

– individuelle Anrufgewohnheiten.

Es wird angeführt, dass Missbrauchserkennungssysteme dataillierte Daten über lange Zeiträume sammeln müssen, um „lernen“ zu können. In der Tat wird berichtet, dass die Qualität der Missbrauchserkennung mit fortschreitender Zeit ansteigt, wenn „Data Mining“-Verfahren und andere vergleichbare Techniken angewandt werden. Dies setzt die Aufbewahrung der gesamten zurückliegenden Verbindungsdaten voraus. Generell nehmen der Umfang der gesammelten Daten und der Zeitraum, in dem diese Daten für Analysezwecke aufbewahrt werden, mit der Komplexität und Anpassungsfähigkeit der Betrugserkennungssysteme zu.

Datenschutzaspekte

Die Missbrauchserkennung birgt verschiedene Datenschutzrisiken. Unschuldige Bürger können als potenzielle Betrüger behandelt werden, es gibt ein Risiko für

falsche Entscheidungen; Daten, die für den Zweck der Missbrauchserkennung verarbeitet werden, können ihrerseits missbraucht werden und die Übermittlung und Nutzung dieser Daten an Dritte (Polizei, Geheimdienste) kann außerhalb der Kontrolle der Betreiber liegen.

Was sind die gesetzlichen Rahmenbedingungen im Hinblick auf die Aktivitäten der Telekommunikationsdiensteanbieter zur Missbrauchserkennung? Die Erkennungsmethoden stützen sich auf die Analyse von Verkehrsdaten, die in einem allgemeinen Sinne als personenbezogene Daten anzusehen sind. Die Verarbeitung von Verbindungsdaten sollte daher den Datenschutzbestimmungen genügen.

Von der Perspektive der Telekommunikationsanbieter aus gesehen eröffnet die Formulierung in den anwendbaren Gesetzen einen Interpretationsspielraum im Hinblick darauf, welche Daten sie rechtmäßig erheben, verarbeiten und speichern können. Dasselbe gilt für die Zeitdauer, für die die Daten gespeichert werden.

Empfehlungen der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

1. Methoden zur Begrenzung des finanziellen Risikos wie Systeme mit vorheriger Bezahlung, die Verkürzung von Abrechnungszeiträumen oder garantierte Zahlungen sind generell den Methoden zur nachträglichen Überwachung oder Analyse des persönlichen Verhaltens vorzuziehen.

2. Die Anwendung von Missbrauchserkennungssystemen sollte auf diejenigen Fälle begrenzt werden, in denen präventive Maßnahmen zur Minimierung des Risikos erwiesenermaßen gescheitert sind. Generell ist die umfassende Aufbewahrung von Verbindungsdaten für verlängerte Zeiträume zum Zwecke der Missbrauchserkennung nicht zu rechtfertigen.

3. Systeme zur Missbrauchserkennung existieren in verschiedener Ausprägung und die Daten, von denen behauptet wird, dass sie für die Missbrauchserkennung erforderlich sind, differieren stark, abhängig von der Art des Betrugs und den für die Betrugserkennung eingesetzten Technologien. Jede Art des Betrugs sollte in der Art behandelt werden, die den Datenschutz am wenigsten einschränkt; z. B. sollte der Betrug durch Kunden durch die Verbesserung von Verfahren zur Überprüfung der Kreditwürdigkeit der Anschlussinhaber begrenzt werden.

4. In Fällen, in denen Missbrauchserkennungssysteme automatisierte Entscheidungen treffen, sollten die Betroffenen darüber informiert werden und Möglichkeiten des Rechtsschutzes erhalten.

27th meeting, 4th and 5th May 2000, Rethymnon, Greece

Common Position on the detection of fraud in telecommunications

The International Working Group on Data Protection in Telecommunications draws attention to the data protection issues related to the detection of telecommunications fraud, in particular concerning the processing of traffic data by telecommunications operators.

Fraud is specifically used here in the sense of "fraudulent use of telecommunications services" rather than "fraudulent activities by means of telecommunications networks (hacking etc.)". The types of telecommunications fraud discussed here are detrimental to the telecommunications operators, as these deliver services which they are not, or only partly being paid for, resulting in loss of revenue.

The size of the fraud phenomenon, in terms of financial damage to operators is hard to estimate. Numbers quoted are 3–6 % of revenue worldwide. It is clear that growing fraud levels must be a concern to many operators, especially since the margins on telecommunications services are dropping in the liberalised markets. There is a vested interest of telecom operators limiting this type of fraud.

General types of fraud

Two general types of fraud are:

Call sell operation/toll fraud. The reselling of calls to third persons without paying the operator for the calls. Several constructions are possible, often using "phone-houses", dial-through constructions or mobile equipment.

Premium Rate Service Fraud. This includes several types of fraud with expensive special tariff numbers (typically 09-numbers). Sometimes the number is exploited in such a way that calls are being made, using fraudulent phones, to a revenue-generating number. A different approach is to have partners in crime connect phones, e.g. after business hours in offices, to such numbers. Another option is that people are, without being aware of this, being lured into making calls to expensive numbers. The fraudster collects the revenues from this activities.

Methods of committing fraud

The main ways of committing fraud are:

Subscriber fraud. A subscription is obtained through the regular subscription process under a false or stolen identity. It is also possible that employees of the

telecom operator participate in this type of fraud, e.g. by deliberately skipping procedures to check a new subscriber's identity.

Surfing. This includes several forms of unauthorised use of facilities.

– Cloning of handsets. Identities, telephones or other attributes are being duplicated.

– Calling card fraud. This includes theft of or fraud with PIN-codes and recharging cards.

– Misuse of hardware. This includes several ways to break into the telecommunications network.

Once this hacking has succeeded the network is used without paying for it. Access to the network can be gained through maintenance ports in telephone exchanges or PBXs, dial-in numbers, voice-mail systems etc.

- Teeing-in other subscriber' s line by physically connecting to the line.

Mobile fraud. Mobile communications open up several new forms of fraud. Specific types of fraud which are committed using mobile phones are the following. The simplest form is plain theft of mobile phones. Roaming fraud another form; expensive calls are being made from a foreign country, making use of the delay in billing these calls in the country where the phone is registered. Recharging or copying prepaid cards is also reported. Several types of fraud of connect-through services exist as well.

Detection of fraud: methods

Fighting fraud implies detection of fraud. In this section some indications will be given as to how fraud-detection works and which data are being used as input for the applied techniques.

Most data used for fraud detection are either Call Detail Records (CDRs) or billing data. CDRs form a collection of data sent over the network through the signalling system. These traffic data contain the calling and receiving number, time, duration and other data necessary for the communication. The billing system is the place where the CDRs are valued and the bills of individual customers are made up.

Fraud detection systems can be roughly grouped as follows:

– Simple analysis of reports based on traffic data (CDRs) and billing data. This means analysing the reports and searching for irregularities.

– Automated tools to analyse CDRs based on fixed pre-set rules. This can be done during the actual communication or afterwards. This offers more flexibility than the plain analysis, with the possibility to adapt rules. These systems are typical 'expert-systems'.

– Complex automated systems, with some capability to learn and create new detection rules itself. Techniques involved are neural networks, genetic algorithms and data warehousing/data mining.

Data used for fraud detection

Several types of data are used as input for fraud detection. A non-limitative summary of the data involved in this process includes:

– High use

– Rising use

– Suspect use, such as suddenly increasing use of Premium Rate Services

– Long calls, e.g. longer than eight hours

– Suspect foreign destinations, which are known to fraud-sensitive

– Use of expensive services known to be fraud-sensitive

– User profiles; generally divided into several risk classes

– Individual calling patterns.

In order to 'learn', it is claimed that fraud detection systems have to assemble detailed data over long periods. In fact, when applying data mining and comparable techniques, the quality of the fraud detection is said to improve as time proceeds. This implies that the full history of subscriptions are being kept.As a rule, the more complex and adaptive the fraud detection system, the more data are being collected, and the longer these are kept for analysis.

Data protection aspects

Fraud detection brings several risks to privacy. Innocent people may be treated as potential fraudeurs, there is a risk of taking wrong decisions, the data processed for the purpose of fraud detection may be misused while the transfer and use of these data to third parties (police, secret services) might be beyond control of the operator.

Given the activities of telecommunications operators in fraud detection, what are the legal boundary conditions? Detection methods rely on the analysis of traffic data, which can in a general sense be considered as personal data. Processing of traffic data should therefore comply to privacy regulations.

Seen from the perspective of telecom operators, the wording in the applicable laws leaves room for interpretation as to which data they can legitimately collect, process and store. The same applies to the duration for which the data are being kept.

Recommendations of the IWGDPT:

1. In general, methods to limit financial risks likes prepaid systems, shortening of billing periods or guaranteed payments are to preferred to methods for afterwards monitoring or analysing personal behaviour.

2. The use of fraud detection systems should be limited to those circumstances where preventive measures to minimize the risks are demonstrated to have failed. No general justification can be given for the overall retention of traffic data for prolonged periods for the purpose of fraud detection.

3. Fraud detection systems come in many forms, and the data claimed to be necessary for the detection of fraud differ widely, dependent on the type of fraud and the technologies applied for detection. Each type of fraud should be dealt with in the way that is the least privacy invasive e.g. subscriber fraud should be limited by improving procedures to check the credentials of the subscriber.

4. In case fraud detection systems create automated decisions the data subject should be informed about that and be given means of redress.

Gemeinsamer Standpunkt zu Infomediaries (Informationsmakler) – eine datenschutzfreundliche Geschäftsidee?

Die Arbeitsgruppe hat seit 1999 die Notwendigkeit betont, technische Mittel zur Verbesserung des Datenschutzes für die Nutzer im Internet zu entwickeln, insbesondere, indem ihnen die Möglichkeit des Netzzuganges eröffnet wird, ohne dass sie ihre Identität preisgeben müssen, wo personenbezogene Daten zur Erbringung eines bestimmten Dienstes nicht erfordlich sind[1]. Die Arbeitsgruppe hat auch

[1] Budapest-Berlin-Memorandum, Bericht und Leitlinien zu Datenschutz und Schutz der Privatsphäre im Internet, <http://www.lda.brandenburg.de/tb/tb5/tb5anl10.htm>

Maßnahmen für die datenschutzfreundliche Gestaltung intelligenter Software Agents empfohlen[2]. Mittlerweile ist eine Geschäftsidee entwickelt und in die Praxis umgesetzt worden, die den Anspruch erhebt, den Nutzern die Möglichkeit zum „Verbergen" ihrer Identität zu eröffnen, während sie im World Wide Web surfen.

John Hagel und Marc Singer haben „Infomediaries" definiert als „Makler oder Vermittlungsinstanzen, die den Kunden helfen, den Wert ihrer Daten zu maximieren"[3]. Nach ihrer Meinung sind Infomediaries besser in der Lage, den Interessen der Nutzer und Kunden zu dienen, als Software Agents. „Viele Verbraucher zögern, … intime Details über ihr Leben irgend jemandem, geschweige denn einem elektronischen Programm zu offenbaren, das ihre Informationen in unangemessener Weise verbreiten könnte, während es sich durch das Netz bewegt." Verkäufer, die unzufrieden mit Software Agents waren, die nur Preise verglichen, fanden Möglichkeiten, sie von ihren Web Sites auszuschließen. Ein Infomediary würde demgegenüber als Agent oder Treuhänder der Kunden handeln und dabei aggressiv deren Interessen vertreten und ihnen helfen, den Gegenwert zu optimieren, den sie von den Verkäufern erhalten. Durch die Aggregation von Daten und die Nutzung der kombinierten Marktmacht zahlreicher Kunden in einer „virtuellen Einkaufsgemeinschaft" würde ein umgekehrter Markt („reverse market") entstehen.

Gleichzeitig sammeln Infomediaries detaillierte Daten von ihren Kunden über deren Wünsche, um die Web Sites finden zu können, die diesen Wünschen am besten entsprechen. Ein Informationsmakler kann nur dann hoffen, ein außerordentlich weitgehendes Profil des einzelnen Kunden zu erhalten, wenn er verspricht, dessen Daten gegen Missbrauch zu schützen und personenbezogene Daten nur mit der ausdrücklichen Erlaubnis des Kunden für Werbezwecke zu offenbaren („permission marketing"). Zu diesem Zweck wird der Informationsmakler sowohl einen „Datenschutz-Werkzeugkasten" als auch einen „Profilbildungs-Werkzeugkasten" anbieten. Der „Datenschutz-Werkzeugkasten" wird anonyme E-Mail-Adressen in Verbindung mit Filtersoftware zur Unterbindung von unerwünschter E-Mail-Werbung (spam) enthalten; er könnte auch technische Hilfsmittel zur Unterdrückung von Cookies („Cookie-Schneider") zur Verfügung stellen oder Cookies im Interesse der Kunden einsetzen, um diesen eine Überprüfung des eigenen Verhaltens online oder der eigenen Einkäufe zu ermöglichen („umgedrehte Cookies"). Der Informationsmakler sollte einen technischen Werkzeugkasten anbieten, um die Privatsphäre seines Kunden zu schützen und um die Verbraucher „in Anonymität zu hüllen"[4].

---

[2] vgl. den Gemeinsamen Standpunkt zu intelligenten Software-Agenten (April 1999) p<http://www.lda.brandenburg.de/tb/tb8/tb8anh.htmxxC2>

[3] Hagel/Singer, Net Worth-Shaping Makets when Customers Make the Rules Havard Business School Press, Boston 1999

[4] Hagel/Singer, ebda. S. 30 und Appendix (S. 261)

Der Profilbildungs-Werkzeugkasten würde andererseits den Aufbau einer sehr viel vollständigeren Übersicht der Transaktionen und Vorlieben des Kunden ermöglichen. Informationsmakler werden sogar Daten über Online-Aktivitäten mit Daten über konventionelle Offline-Geschäfte (z. B. unter Einsatz einer Kreditkarte) verknüpfen können. Diese Profile können dynamisch sein, d. h. sie entwickeln sich durch die Aktivitäten von Kunden mit ähnlichen Nutzungsprofilen und Präferenzen. Außerdem können den Kunden Profile über Verkäufer im Netz zur Verfügung gestellt werden, wodurch die Kunden Informationen über die Zahl der Verkäufe (z. B. eines bestimmten Computertyps) unter Einschaltung eines Informationsmaklers und über die Zahl der Beschwerden oder umgetauschten Produkte erhalten würden.

Der Kunde eines Infomediaries hat die Wahl, entweder anonym zu bleiben oder die Weitergabe seines Profils und seiner personenbezogenen Daten an Verkäufer oder werbetreibende Unternehmen zuzulassen. Im zuletzt genannten Fall erhält der Kunde entweder kleinere Barbeträge, Rabatte beim Preis gekaufter Produkte, billigeren oder kostenlosen Netzzugang oder andere Vorteile. Kunden, die sich dazu entschließen, vollständig anonym zu bleiben, erhalten für den Verzicht auf die Barzahlungen oder anderen Vorteile die Zusage, das ihre Privatsphäre geschützt bleibt.

Eine Reihe von Infomediaries sind bereits im Netz tätig, die diese Geschäftsidee mit gewissen Modifikationen verfolgen. Sie bieten Dienste an, die vom Kinderschutz im World Wide Web (PrivaSeek) bis zur Online-Partnerschaftsvermittlung (yenta.com; flirtmaschine.de) reichen. Einige bieten elektronische Brieftaschen (electronic wallets) an, die es dem Nutzer erlauben, personenbezogene Daten einmal in ein Formular einzutragen und die Offenbarung dieser Daten zu kontrollieren.

Empfehlungen

Es ist im Grundsatz zu begrüßen, dass Datenschutz und der Schutz der Privatsphäre an Bedeutung im Marktgeschehen gewinnen und von einigen jungen Internet-Unternehmen als lukrative Geschäftsidee angesehen werden. Allerdings muss der Verbraucher effektive Rechtsschutzmöglichkeiten haben, falls seine Daten vom Informationsmarkler nicht in der versprochenen Weise genutzt werden. Eine Geschäftsidee kann Rechtsansprüche der Betroffenen nicht ersetzen, aber sie ist ein positives Beispiel für die Umsetzung eines bestehenden rechtlichen Rahmens mit Hilfe der Kräfte des Marktes.

Es muss der freien Entscheidung der Betroffenen überlassen bleiben, ob sie das Recht zur Nutzung ihrer personenbezogenen Informationen verkaufen wollen. Einige Infomediaries (z. B. Partnerschaftsvermittlungen) verwenden extrem sensible Informationen. Darüber hinaus sind Betroffene nicht immer

Verbraucher; sie können sich z. B. an politische Aktivitäten im Netz beteiligen und müssen sorgfältig abwägen, ob sie sich dabei eines „Agenten“ bedienen wollen.

Die Fähigkeit von Infomediaries zur Profilbildung unterstreicht die Bedeutung des Vertrauens in der Beziehung zum Kunden. Dies ist vergleichbar mit der Beziehung zwischen einem Anwalt und seinem Mandanten oder der besonders vertrauensvollen Beziehung zwischen Ärzten und Patienten; die Gesetzgeber sollten prüfen, ob diese Beziehung entsprechend gegen Durchsuchung und Beschlagnahme geschützt werden muss.

Schließlich müssen Infomediaries bei Aufbau von Persönlichkeitsprofilen die Grundsätze beachten, die die Arbeitsgruppe in ihrem gemeinsamen Standpunkt zu Online-Profilen im Internet am 5. Mai 2000 beschlossen hat (<http://www.privacy.de/doc/int/iwgdpt/pr_en.htm>).

Common Position on Infomediaries – a privacy-friendly business model?

The Working Group has since 1996 stressed the need to develop technical means to improve the user’s privacy on the Internet, especially giving the opportunity to access the Internet without revealing their identity where personal data are not needed to provide a certain service[1]. The Group has also recommended measures for a privacy-friendly design of intelligent software agents[2]. In the meantime a business model has been developed and put into practice which claims to give users the option to “mask” their identity while surfing the Web.

John Hagel and Marc Singer have defined infomediaries as “brokers or intermediaries that help customers to maximise the value of their data”[3]. Infomediaries in their view are better equipped than software agents to serve the user‘/customer’s interests. “Many consumers are hesitant to di- vulge…intimate details about their lives to anybody let alone an electronic entity that might expose their information inappropriately as it crawls across the Web .”[4] Vendors who were dissatisfied with software agents that only compared prices found ways to block them from their Web sites. An infomediary on the other hand would act as an agent or custodian

[1] Cf. Budapest-Berlin Memorandum, Report and Guidance on Data Protection and Privacy on the Internet, http://www.datenschutz-berlin.de/doc/int/iwgdpt/bbmem_en.htm

[2] Cf. Common Position on Intelligent Software Agents (April 1999) http://www.datenschutz-berlin.de/doc/int/iwgdpt/agent_en.htm

[3] Hagel/Singer, Net Worth – Shaping Markets When Customers Make the Rules, Harvard Business School Press, Boston 1999

[4] Hagel/Singer, ibid., p. 27

on behalf of their clients aggressively representing their interests and helping them to optimize the value they receive from vendors. By aggregating information and using combined market power of numerous customers in a "virtual shopping club" infomediaries would create a "reverse market".

At the same time infomediaries will collect detailed information from their customers about their preferences in order to be able to find the Web sites which suit them best. An infomediary – according to Hagel/Singer – can only hope to get an extraordinarily deep and broad informational profile of the individual customer if it pledges to protect this information against abuse and to disclose personal data only with the customer's specific permission ("permission marketing"). To this end the infomediary will offer both a "privacy tool kit" and a "profiling tool kit". The privacy tool kit will include anonymous e-mail addresses linked with filtering software in order to block spam; it could also provide for cookie suppression techniques such as "cookie cutters" or use cookies for customers to keep track of their own online behaviour or purchases ("reverse cookies"). The infomediary should offer a technology tool kit in order to protect its client's privacy and to "cloak customers in anonymity"[5].

The profiling tool kit on the other hand would allow the build-up of a much more complete and integrated view of customer transactions and preferences. Infomediaries will even be able to link information about online activities with information concerning conventional offline transactions (e.g. by using a credit card). These profiles may be dynamic, i.e. they develop through the activities of customers with similar profiles and preferences. Similarly profiles about vendors may be made available to the clients giving them information about the number of transactions through infomediary services (e.g. computer of a certain type sold) and the number of complaints or products returned to the vendor.

The customer of an infomediary has the choice either to remain anonymous or to allow his profile and his personal data to be given to vendors or direct marketers. In the latter case the customer will receive either small cash payments, a discount in the product price, cheaper or free Internet access or other benefits. Customers who choose to remain entirely anonymous will forgo these payments or benefits in return for the assurance of their privacy.

A number of infomediaries are already operating on the Web following this business model with certain modifications. They offer services ranging from child protection on the web (PrivaSeek) to online matchmaking (yenta.com; flirtmaschine.de). Some offer electronic wallets which allow the user to fill in personal information in forms and to control the release this information.

[5] Hagel/Singer, ibid., p.30 and Appendix (p. 261)

Recommendations:

1. It is to be welcomed in principle that privacy is gaining ground in the market and is taken up by some Internet startups as a business case. However, the consumer needs effective legal recourse in case his data are not used as promised by the infomediary. A business model cannot replace legal rights for data subjects but it is a positive example for implementing an existing legal framework through market forces.

2. It must remain the free decision of the data subjects whether they wish to sell the right to use their personal information. Some infomediaries (e.g. matchmakers) handle extremely sensitive information. In addition, data subjects are not always consumers; they may participate e.g. in political activities on the web and have to consider carefully whether to engage an agent in doing so.

3. The profiling capability of infomediaries points to the importance of trust in the relationship with the client. This resembles the client-attorney relationship or the trusted relationship between doctors and their patients and legislators should consider to protect it against search and seizure accordingly.

4. Finally, infomediaries when building up personal profiles must respect the principles adopted by the Working Group in their Common Position regarding Online Profiles on the Internet on 5 May 2000.

Gemeinsamer Standpunkt zu Datenschutz und Urheberrechts-Management

Das Urheberrecht und das Recht auf Datenschutz sind schon immer als aus den gleichen Wurzeln stammend betrachtet worden. Warren und Brandeis haben sich, als sie die Grundlagen des „Rechts auf Privatheit“[1] des Einzelnen legten, auf die allgemeinen Gesetze zum Schutz geistigen Eigentums bezogen. Trotzdem scheinen im Rahmen des elektronischen Geschäftsverkehrs über das Internet Urheberrecht und Datenschutz zu kollidieren.

Während in der analogen „Offline-Welt“ Urheberrechtsgesetze Ausnahmen für die private (nicht-kommerzielle) Nutzung enthielten, umfasst das Urheberrecht in der digitalen (online) Welt jede Handlung der temporären Reproduktion und der Übermittlung in den Arbeitsspeicher eines Computers zum Zwecke des Lesens, Zuhörens oder Ansehens[2]. Der Autor eines digitalen Werks (einschließlich

[1] Warren/Brandeis, Harvard Law Review Vol. IV (1890), 193, 204

[2] Bygrave/Koelman, Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems, 1998 [http://www.imprimatur.alcs.co.uk/imp_ftp/privreportdef.pdf]

Software und Datenbanken) hat das Recht, dies zu verbieten oder für jede solche Nutzung eine Gebühr zu erheben.

Das praktische Problem mag teilweise der Tatsache zuzurechnen sein, dass es bisher keine verlässlichen datenschutzfreundlichen Zahlungsmittel im Internet gibt. Wenn einem anonyme Zahlungsmethoden angeboten werden, könnten digitale Werke zum Download oder zur Nutzung gegen sofortige Bezahlung zur Verfügung gestellt werden.

Für den legitimen Zweck des Schutzes des geistigen Eigentums im Cyberspace und zur Abwehr von Software-Piraterie werden Technologien wie Roboter („web spiders") geschützte Objekte oder digitale Werke identifizieren, die Nachrichten an zentrale Server mit der Aufforderung zur Erteilung der Zugriffserlaubnis oder zur Bezahlung zu zentralen Servern schicken, wenn sie genutzt oder kopiert werden. Elektronische Copyright-Management-Systeme (ECMS), die zur allgegenwärtigen Überwachung von Nutzern digitaler Werke führen könnten, werden entwickelt und angeboten. Einige ECMS überwachen jede einzelne Handlung des Lesens, Anhörens und Betrachtens im Internet durch individuelle Nutzer, wobei hoch sensible Informationen über die Betroffenen gesammelt werden[3].

ECMS werden weniger von individuellen Inhabern von Urheberrechten, sondern mehr von großen Verlagshäusern und Vermittlern (Vertretern der Rechteinhaber) verwendet, die ein starkes Interesse an der Überwachung des Nutzerverhaltens für Zwecke haben, die nichts mit dem Urheberrechtsschutz zu tun haben (z. B. Direktwerbung). Im Gegensatz dazu speichert in der analogen Welt niemand personenbezogene Daten darüber, wer welches Buch wie oft liest. Hier stehen nicht nur der Datenschutz, sondern auch das Recht auf Informationsfreiheit und freie Meinungsäußerung auf dem Spiel.

Zunehmend wird „Rights Management Information" (RMI) für Zwecke des Urheberrechtsschutzes genutzt. Dazu gehören digitale Wasserzeichen oder andere Techniken, die einen Urheberrechtsgegenstand identifizieren. Diese Information ist durch Bestimmungen des WIPO-Vertrags über Urheberrechte von 1996, die auf die Abwehr der Umgehung von Urheberrechtsschutzmaßnahmen abzielen, geschützt. Allerdings können Rechte-Management-Informationen selbst personenbezogene Daten enthalten, z. B. wenn sie die Identität des Nutzers/Käufers oder die Bedingung einer personalisierten Linzenz enthalten. Daher können sie zur Erhebung und Verbreitung persönlich identifizierender Informationen über die Online-Aktivitäten eines Einzelnen genutzt werden.

[3] Für eine detaillierte Analyse der verfügbaren Technologien siehe Greenleaf, „IP Phone Home", ECMS, c-Tech, and Protecting Privacy Against Surveillance by Digital Works, Proceedings of the 21 International Conference on Privacy and Personal Data Protection, Hong Kong 1999, [http://www2.austlII.edu.au/~graham/publications/ip_privacy/]

Versuche, solche Informationen zu löschen oder Roboter („web spiders“) an der Suche nach solchen Informationen sogar für Zwecke der Direktwerbung zu verhindern, könnten als eine illegale Umgehung von Urheberrechtstechnologien angesehen werden.

Die Überwachung des „Weges“ digitaler Werke kann zum Entstehen eines personenbeziehbaren Nutzerprofils führen. Die Verhinderung des Zugriffs auf urheberrechtlich geschützte Objekte insgesamt, z. B. durch die Nutzung von Verschlüsselung, könnte aus Sicht des Datenschutzes vorzuziehen sein, solange dies nicht im Gegenzug zu einer Registrierung des Nutzerverhaltens führt. Nationale Systeme zur Verhinderung der Veröffentlichung illegaler Inhalte werden beraten, die dem Durchsuchungs- und Beschlagnahme-Modell an Landesgrenzen nachgebildet sind und die nicht nur zur Verhinderung der Verletzung von Urheberrechten verwendet werden könnten, sondern auch zum Auffinden von Material im Cyberspace, das unter dem anwendbaren nationalen Recht illegal ist. Allerdings könnte dies zu einer Aushöhlung des Telekommunikationsgeheimnisses führen und dürfte wegen der Architektur des Internet wenig effektiv sein.

Um einen gerechten Ausgleich zwischen dem Datenschutz der Nutzer und den Rechten der Urheber zu erreichen, ruft die Arbeitsgruppe Planer, Produzenten und Anbieter von ECMS auf,

a) elektronische Copyright-Management-Systeme zu entwickeln, zu produzieren und anzubieten, die keine personenbezogenen Daten erheben und die anonyme oder pseudonyme Transaktionen erlauben. Die Arbeitsgruppe unterstreicht in diesem Zusammenhang die Ansicht, dass die Nutzer generell die Möglichkeit haben sollten, auf das Internet ohne Preisgabe ihrer Identität zuzugreifen, sofern personenbezogene Daten nicht für die Erbringung eines bestimmten Dienstes erforderlich sind[4]. Unter bestimmten Bedingungen kann die Nutzung von Pseudonymen die Privat-sphäre der Nutzer und zugleich die ökonomischen Interessen der Inhaber von Urheberrechten schützen: Digitale Wasserzeichen könnten Transaktions-Codes enthalten, durch die einzelne Kopien nummeriert und diese Nummern mit Angaben über die einzelnen Nutzer in eine sichere Datenbank verbunden werden, die z. B. von einem vertrauenswürdigen Dritten betrieben wird. Diese Verbindung sollte nur zum Zwecke des Schutzes von Urheberrechten z. B. aufgrund eines Gerichtsbeschlusses zugänglich gemacht werden;

b) die Nutzer über die Verarbeitung personenbezogener Daten (einschließlich Pseudonyme) durch digitale Werke zu informieren und für die größtmögliche Transparenz beim Betrieb der Copyright-Management-Systeme zu sorgen.

[4] Budapest-Berlin-Memorandum vom 19.11.1996, Empfehlungen 6 und 9

Die Arbeitsgruppe unterstützt die Empfehlung 1/99 der Europäischen Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware[5]. Dies gilt auch für die Verarbeitung personenbezogener Daten durch digitale Werke.

Filter- und Überwachungstechniken zur Überwachung von Inhalten gefährden den Datenschutz und das Telekommunikationsgeheimnis. Die Arbeitsgruppe hält sie daher für die Abwehr der Verletzung von Urheberrechten nicht für angemessen.

Der datenschutzfreundliche Schutz des geistigen Eigentums ist unverzichtbar für die Entwicklung des globalen elektronischen Geschäftsverkehrs. Daher sind sowohl eine internationale Regelung im Rahmen der WIPO wie auch Standardisierungsmaßnahmen notwendig, um die Probleme des grenzübergreifenden Schutzes von Urheberrechten unter Nutzung datenschutzfreundlicher Technologien zu lösen.

Common Position on Privacy and Copyright Management

Copyright and the right to privacy have always been considered to have the same roots. Warren and Brandeis referred to the common law on the protection of intellectual property when laying the foundations for the individual's "right to privacy"[1]. And yet in the framework of electronic commerce via the Internet copyright and privacy seem to collide.

Whereas in the analogous (offline) world copyright law provided for exemptions for private (non-commercial) use in the digital (online) world copyright law covers every act of temporary reproduction and transfer to a computer's Random Access Memory for the purpose of reading, listening or viewing[2]. The author of a digital work (including software programs, databases) has the right to forbid this or to charge for any such use.

Partly the practical problem may be attributed to the fact that there are so far no reliable privacy-friendly methods of payment on the Internet available. Once

[5] [http://www.privacy.de/doc/eu/gruppe29/wp17_en.htm]

[1] Warren/Brandeis, Harvard Law Review Vol. IV (1890), 193, 204

[2] Bygrave/Koelman, Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems, 1998, http://www.imprimatur.alcs.co.uk/imp_ftp/privreportdef.pdf

methods of anonymous payment will be offered digital works could be provided for use or download in return for just in time payment.

For the legitimate purpose of protecting intellectual property in cyberspace and to prevent software piracy copyright protection technologies such as robots ("web spiders") will identify protected items or digital works which send reports to central servers when used or copied asking for permission or billing. Electronic Copyright Management Systems (ECMS) are being devised and offered which could lead to ubiquitous surveillance of users by digital works. Some ECMS are monitoring every single act of reading, listening and viewing on the Internet by individual users thereby collecting highly sensitive information about the data subject concerned[3].

ECMS will be run not so much by individual copyright-holders but by large publishing houses and intermediaries (representatives of rights-holders) who have a strong interest in monitoring user behaviour for secondary purposes not related to copyright protection (e.g. direct marketing). By contrast in the analogous world no one is storing personal data about who is reading which book how many times. Not only privacy but also freedom of speech and information are at stake here.

Increasingly rights management information (RMI) is being used for copyright purposes. This includes digital watermarks or other techniques identifiying the copyright item. This information is in turn protected against removal by provisions of the WIPO Copyright Treaty 1996 which are aimed at preventing circumvention of copyright protection. However, rights management information may in itself be personal information e.g. if it contains the identity of the user/purchaser or conditions of a personalized licence. Therefore it can be used to collect and disseminate personally identifying information on an individual's online activities.

Attempts to delete such information or to prevent robots ("web spiders") from looking for such information even for direct marketing purposes could be seen as illegal circumvention of copyright technologies.

Monitoring the "flow" of digital works can create a personally identifiable audit trail. Blocking access to copyright items altogether e.g. by using encryption could be preferable from a privacy perspective as long as this does not in turn lead to the registration of user behaviour. National systems to block certain illegal content following the search-and-seizure-model on borders are under consideration

[3] For a detailed analysis of available technologies see Greenleaf, „IP Phone Home", ECMS, c-Tech, and Protecting Privacy Against Surveillance by Digital Works, Proceedings of the 21 International Conference on Privacy and Personal Data Protection, Hong Kong 1999, http://www2.austlII.edu.au/~graham/publications/ip_privacy/

which could be used not only to prevent copyright infringements but also access to material in cyberspace which is illegal under the relevant national law. However, this could lead to inroads into telecommunications secrecy and – due to the architecture of the Internet – this is unlikely to be effective.

In order to strike a fair balance between copyright-holders and users' privacy the Working Group calls on designers, producers and providers of ECMS to

a) Design, produce and provide Electronic Copyright Management Systems, which do not collect personal information and which allow for anonymous or pseudonymous transactions. The Working Group reaffirms in this context the view that in general users should have the option to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service[4]. Under certain conditions the use of pseudonyms could protect user privacy while at the same time preserving the economic interests of copyright-holders: Digital watermarks could contain transaction codes whereby individual copies are numbered and these numbers would be linked to individual users in a secure database run e.g. by a trusted third party. That link should only be made for copyright protection purposes e.g. once a court order had been issued;

b) inform users about the processing of personal data (including pseudonyms) by digital works and provide for the greatest possible transparency in the operation of the copyright management system. The Working Group supports the Recommendation 1/99 adopted by the European Working Party on the Protection of Individuals with regard to the Processing of Personal Data on Invisible and Automated Processing of Personal Data on the Internet Performed by Software and Hardware[5]. This applies equally to the processing of personal data by digital works.

Filtering and scanning techniques to monitor content lead to inroads into privacy and telecommunications secrecy. The Working Group therefore does not consider them to be appropriate for preventing copyright infringements.

The privacy-friendly protection of intellectual property is essential for the development of global electronic commerce. Therefore an international agreement e.g. within the framework of WIPO as well as standardisation measures are needed to solve the problems of transborder copyright protection using privacy-enhancing technologies.

[4] Budapest-Berlin-Memorandum of 19.11.1996, Recommendations 6 and 9

[5] http://www.privacy.de/doc/eu/gruppe29/wp17_en.htm

Gemeinsamer Standpunkt zu Online-Profilen im Internet

1. Internet-Diensteanbieter sollten ihre Nutzer über Art, Umfang, Ort, Speicherungsdauer und die Zwecke der Speicherung, Verarbeitung und Nutzung ihrer Daten für Profilbildungszwecke informieren. Diese Information sollte auch in den Fällen gegeben werden, in denen Daten unter Verwendung von Pseudonymen oder von noch nicht personalisierten Identifikationsnummern erhoben werden.

2. Die Nutzer müssen von den Anbietern von Profilbildungsdiensten vor dem Setzen von Cookies zum Zwecke der Profilbildung informiert werden.

3. Den Nutzern muss ein Wahlrecht hinsichtlich der Verarbeitung ihrer Daten eingeräumt werden (wenigstens ein Widerspruchsrecht). In diesem Fall müssen die Diensteanbieter den Nutzern garantieren, dass Daten über ihr Nutzungsverhalten im Internet nicht zum Aufbau von Nutzerprofilen durch technische Einrichtungen genutzt werden.

4. Die Nutzer sollen das Recht haben, eine Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

5. Eine Personalisierung von Nutzerprofilen setzt die vorherige informierte Einwilligung des Nutzers voraus („opt in“).

6. Die Arbeitsgruppe hält es für unverzichtbar, dass die Einhaltung von Datenschutzbestimmungen bei Profilbildungsdiensten durch unabhängige Stellen verifiziert werden kann.

7. Den Nutzern sollte das Recht eingeräumt werden, jederzeit ihr Nutzerprofil bei dem Anbieter kostenfrei einzusehen. Anbieter von Profilbildungsdiensten müssen die Möglichkeit zum Online-Zugriff des Nutzers auf die über ihn gespeicherten Daten sicherstellen. Sofern das Profil unter Verwendung von Pseudonym erstellt wird, sollten die Nutzer die Möglichkeit zur Auskunft über ihre Daten sowie zur Berichtigung und Löschung ihrer Daten haben, ohne dabei ihre Identität offenbaren zu müssen.

8. Anbieter von Profilbildungsdiensten müssen angemessene Sicherungsmaßnahmen treffen.

Common Position regarding Online Profiles on the Internet

1. Internet service providers should notify users about the type, scope, place, duration of storage and purposes of collection, processing and use of their data for profiling purposes. This information should be given even in the case, that data are collected using pseudonyms or not yet personalized identification numbers.

2. Users must be informed by profiling services before setting of cookies used for profiling.

3. Users must be given a right to choose about the processing of their data (at least "opt out"). In this case providers have to guarantee the users, that the data about their recent use of the Internet is not used to build up profiles by technical means.

4. Users should have a right to withdraw their consent at any time with effect for the future.

5. Personalization of user profiles requires users' informed prior consent ("opt in").

6. The Working Group considers independent verification of privacy compliance of profiling services by independent bodies to be essential.

7. Users should have the right to inspect, free of charge, their profiles at the provider's site at any time. Profiling Services have to provide for online access to the user's data stored. If the profile is collected using pseudonyms, users should have the opportunity to access, correct and delete their data without disclosing their identity.

8. Adequate security measures have to be taken by the profiling service providers.

Gemeinsamer Standpunkt zu Datenschutzaspekten bei der Registrierung von Domain-Namen im Internet

Mit der zunehmenden Nutzung des Internet registrieren immer mehr Privatpersonen eigene Domain-Namen bei den verschiedenen nationalen und internationalen Network Information Centers (NICs). Bei der Registrierung eines Domain-Namens erheben die NICs personenbezogene Daten von den Antragstellern (z. B. Name, Adresse und Telefonnummer), die regelmäßig in so genannten „WhoIs-

Datenbanken“ im Internet verfügbar gemacht werden. In den meisten Ländern wird in den Geschäftsbedingungen der jeweiligen NICs die Erhebung und Veröffentlichung dieser Daten für die Registrierung eines Domain-Namens zur Bedingung gemacht.

Während diese Datenbanken ursprünglich dazu bestimmt waren, die technische Verwaltung des Netzes zu ermöglichen (z. B. um den Betreiber einer Domain ausfindig zu machen, die durch Fehlfunktion das Funktionieren des Netzes beeinträchtigt), hat die Entwicklung des Netzes zum technischen Rückgrat der sich entwickelnden „Informationsgesellschaft“ neue Interessen verschiedener Gruppen an einer Nutzung dieser Daten entstehen lassen:

Strafverfolgungsbehörden nutzen die Datenbanken, um Betrug und die Veröffentlichung illegaler Inhalte im Netz zu bekämpfen.

In der jüngeren Vergangenheit hat die World Intellectual Property Organisation (WIPO) einen Bericht an die „Internet Corporation for Assigned Names and Numbers“ (ICANN) über Urheberrechtsfragen bei der Verwaltung von Internet-Namen und -Adressen publiziert. WIPO hat unter anderem vorgeschlagen, personenbezogene Daten von jedem Inhaber einer second level domain in die generic Top Level Domains (gTLD) aufzunehmen und sie in einer öffentlich zugänglichen Datenbank im Internet zu veröffentlichen, um es den Inhabern von Urheberrechten und Markenrechten im Falle der Verletzung dieser Rechte durch einen Domain-Inhaber zu ermöglichen, die verantwortliche Person aufzufinden und mit ihr in Kontakt zu treten.

Dieser Ansatz findet sich auch in ICANN’s Erklärung zur „Registrar Accreditation Policy“ wieder, die Registrare von Domain-Namen in den generic Top Level Domains verpflichtet, Adressdaten ihrer Kunden zu erheben und diese Daten in Echtzeit öffentlich zugänglich zu machen (z. B. durch Einrichtung eines WhoIs-Service.

Gleichzeitig kann die Veröffentlichung von Namen und Adressen eines Domain-Inhabers auch für jeden Internetnutzer nützlich sein, dessen Datenschutzrechte durch Veröffentlichung personenbezogener Daten auf einer Website oder durch die Nutzung personenbezogener Daten durch einen Domain-Inhaber verletzt wurden. Nicht in jedem Land existiert eine Verpflichtung für die Diensteanbieter, ihren Namen und ihre Adresse auf Ihrer Website zu veröffentlichen. Daher kann die Veröffentlichung dieser Daten durch die nationalen NICs eine Voraussetzung für den Nutzer sein, um seine Datenschutzrechte gegenüber einem Diensteanbieter wahrzunehmen.

Trotzdem wirft die Erhebung und Veröffentlichung personenbezogener Daten von Domain-Inhabern selbst ebenfalls Datenschutzprobleme auf.

Das Erfordernis zum Schutz des Einzelnen ist seit mehr als 20 Jahren sowohl in den existierenden nationalen Datenschutzgesetzen als auch in der internationalen Gemeinschaft anerkannt worden (z. B. in den Datenschutzrichtlinien der OECD von 1980, im Übereinkommen des Europarats Nr. 108 und in jüngerer Zeit auch in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr). Diese Regelungen enthalten gemeinsame Grundprinzipien zum fairen Umgang mit personenbezogenen Daten. Zu diesen Prinzipien gehören die Verpflichtung, die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten zu informieren, das Prinzip der Beschränkung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf das für den definierten Zweck unverzichtbare Maß und der Schutz gegen unbefugte zweckfremde Nutzung.

Die Bedeutung des Datenschutzes für die fruchtbare Entwicklung der globalen Informationsgesellschaft ist auch in den Basisdokumenten zur Entwicklung des elektronischen Geschäftsverkehrs anerkannt worden, z. B. in dem „Framework for Global Electronic Commerce“ der USA, der gemeinsamen Erklärung der USA und der Europäischen Union zum elektronischen Geschäftsverkehr, der Europäischen Initiative zum elektronischen Geschäftsverkehr und der Ministerkonferenz der OECD in Ottawa im Oktober 1998.

Das von ICANN entwickelte Registrar Accreditation Agreement (RAA) verwirklicht das Ziel des Schutzes personenbezogener Daten von Domain-Inhabern nicht in hinreichender Weise. Die Arbeitsgruppe empfiehlt daher, folgende Punkte in zukünftigen Fassungen des RAA zu behandeln:

Es ist unverzichtbar, die Zwecke, zu denen die personenbezogenen Daten von Domain-Inhabern erhoben und veröffentlicht werden, zu spezifizieren.

Der Umfang der erhobenen und im Rahmen der Registrierung eines Domain-Namens veröffentlichten Daten sollte auf das absolut notwendige Maß zur Erfüllung des angegebenen Zwecks beschränkt werden. In dieser Hinsicht hat die Arbeitsgruppe Bedenken gegen die zwangsweise Veröffentlichung jeglicher Daten, die über den Namen (der auch der Name eines Unternehmens und nicht einer natürlichen Person sein kann), die Adresse und die E-Mail-Adresse hinausgeht, wenn der Domain-Inhaber nicht selbst für die technische Verwaltung der Domain verantwortlich ist, sondern dies durch einen Diensteanbieter erledigen lässt (wie es bei vielen Privatpersonen, die einen Domain-Namen registriert haben, der Fall ist).

Darüber hinausgehende Daten (besonders Telefon- und Faxnummer) – obwohl sie durch das Register erhoben werden könnten, wenn dies für die Erfüllung von dessen Aufgabe erforderlich ist – sollten sich in solchen Fällen entweder auf den

jeweiligen Diensteanbieter beziehen oder nur mit der ausdrücklichen Einwilligung des Betroffenen veröffentlicht werden. Die zwangsweise Veröffentlichung von Telefon- und Faxnummern von Domain-Inhabern stellt in den Fällen, in denen Privatpersonen Domain-Namen registrieren, ein Problem dar, da es sich bei der entsprechenden Nummer um ihre Privatnummer handeln kann. Das Recht, Telefonnummern nicht zu publizieren – wie es in den meisten nationalen Datenschutzregelungen zur Telekommunikation anerkannt ist -, sollte für die Registrierung eines Domain-Namens nicht abgeschafft werden.

Gleichzeitig sollte jede zweckfremde Nutzung, die mit dem angegebenen Zweck unvereinbar ist (z. B. Werbung), auf die informierte Einwilligung des Betroffenen gestützt werden. In dieser Hinsicht ist das Datenschutzniveau des gegenwärtigen RAA nicht hinreichend (vgl. II.F.6.f).

Darüber hinaus müssen technische Einrichtungen, die den Zugriff auf die von den Betroffenen erhobenen Daten ermöglichen, Sicherungseinrichtungen zur Verwirklichung der Zweckbindung und der Verhinderung unbefugter zweckfremder Verwendung der Daten des Registranten enthalten. Diese Forderung wird durch viele gegenwärtig existierende WhoIs-Datenbanken nicht erfüllt, die unbegrenzte öffentlich zugängliche Suchmöglichkeiten beinhalten. In dieser Hinsicht begrüßt die Arbeitsgruppe die entsprechenden Vorschläge von WIPO in dem Bericht über den Internet-Domain-Name-Prozess, Adressdaten von Domain-Inhabern nur für begrenzte Zwecke zugänglich zu machen und Maßnahmen zu ergreifen, um die unbefugte Zweckentfremdung z. B. für Werbezwecke zu verhindern. Die Arbeitsgruppe hält es für nötig, dass Filtermechanismen in die Schnittstellen zum Zugriff auf die Datenbanken integriert werden, um die Zweckbindung sicherzustellen.

Die Arbeitsgruppe empfiehlt darüber hinaus, dass die Register – da eine global verbindliche Datenschutzgesetzgebung nicht existiert – einen einheitlichen Standard für die Erhebung und Nutzung personenbezogener Daten von Domain-Inhabern einschließlich Regelungen über die Information der Betroffenen über die Zwecke der Erhebung und Nutzung ihrer personenbezogenen Daten und ein Recht auf Auskunft und Berichtigung ihrer Daten entwickeln. Die Einhaltung dieser Regelungen sollte durch Zertifizierungsmechanismen sichergestellt werden.

Die Arbeitsgruppe betont, dass jede Registrierungsinstanz, die innerhalb des Geltungsbereichs existierender Datenschutzgesetze tätig ist, und jegliches nationale Verfahren zur Registrierung von Domain-Namen den existierenden nationalen Gesetzen zum Datenschutz und der Kontrolle durch die jeweiligen Datenschutzbeauftragten unterliegen. Gleichzeitig unterstützt die Arbeitsgruppe die Bemühungen der Europäischen Kommission, den Schutz personenbezogener Daten in einem funktionierenden Internet-Domain-Name-System zum Wohle aller Bürger

zu verstärken, und ermutigt die Europäische Kommission, ihre Beratungen mit ICANN, der US-Regierung und anderen Parteien fortzusetzen.

Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet

With the growing use of the Internet more and more private persons are starting to register their own domain names with the different national and international Network Information Centers (NICs). In the course of the registration of a domain name, the NICs are collecting personal data from the applicants (like name, address and telephone number) which are regularly made publicly available in the so-called "WhoIs-databases" on the Net. In most countries, the collection and publication of these data is mandatory to register a domain name due to the service conditions of the respective NICs.

While these databases were originally intended to facilitate the technical maintenance of the network (e.g. to contact the person running a domain which produced errors hindering the functioning of the net), the development of the net towards the technical backbone of the emerging "Information Society" has created new interests of different parties in the use of these data:

Law enforcement agencies are using the databases for fighting fraud and the publication of illegal material on the net.

More recently, the World Intellectual Property Organisation (WIPO) has published a report to the "Internet Corporation for Assigned Names and Numbers" (ICANN) on Intellectual Property issues in the management of Internet names and addresses. WIPO has among other things suggested to collect personal data from every domain name holder of a second level domain in the generic Top Level Domains (gTLD) and the publication of these data in a publicly accessible database on the Internet to enable holders of copyrights and trademarks to find out and contact the responsible person in cases of a violation of these rights by a domain name holder.

This approach is also reflected in ICANN's Statement of Registrar Accreditation Policy which demands registrars for domain names in the generic Top Level Domains to collect contact details from their applicants and provide public access to these data on a real-time basis (such as by way of a WhoIs service).

At the same time the publication of name and address of a domain name holder can also be useful for any Internet user who has experienced an infringement of his or her privacy through personal data published on a website or the use of

personal data by a domain name holder. An obligation to publish name and address of the holder of an Internet-Service on its website does not exist in every country. Thus, the publication of these data by the national NICs can be a prerequisite for the user in order to exercise his right to privacy against a service provider.

Nevertheless, the collection and publication of personal data of domain name holders gives itself rise to data protection and privacy issues.

The necessity to protect individuals has been recognised for more than twenty years in the existing national data protection regimes as well as in the international community (e.g. in the OECD guidelines on Privacy of 1980, the Council of Europe Convention No. 108, and, more recently, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). These regulations outline similar basic principles on the fair processing of personal information. Among these principles are the obligation to inform the data subjects about the processing of their personal data, the principle of limiting the collection and use of personal data to what is essential to the purpose specified and protection against unauthorised secondary uses.

The importance of the protection of privacy for the fruitful development of the Global Information Society has also been recognised in the basic documents on the development of Electronic Commerce; e.g. in the US "Framework for Global Electronic Commerce" of , the joint EU-US statement on Electronic Commerce, the European Initiative for Electronic Commerce, and at the October 1998 OECD Ministerial Conference in Ottawa.

The current Registrar Accreditation Agreement (RAA) developed by ICANN does not reflect the goal of the protection of personal data of domain name holders in a sufficient way. The Working Group therefore recommends that the following topics be addressed in future versions of the RAA:

It is essential that the purposes of the collection and publication of personal data of domain name holders are being specified.

The amount of data collected and made publicly available in the course of the registration of a domain name should be restricted to what is essential to fulfil the purpose specified. In this respect the Working Group has reservations against a mandatory publication of any data exceeding name (which might also be the name of a company and not of a natural person), address and e-mail-address in cases where the domain name holder is not himself responsible for the technical maintenance of the domain but has this done through a service provider (as is the case with many private persons who have registered domain names).

Any additional data (especially telephone and fax number) – although they might be collected by the registry as necessary with respect to its task – should in such cases either refer to the respective service provider or only be made available with the explicit consent of the data subject. Mandatory publication of telephone and fax numbers of domain name holders would be a problem when private persons register domain names, where the number to be provided might be their home number. The right not to have telephone numbers published – as recognised in most of the national telecommunications data protection regimes – should not be abolished when registering a domain name.

At the same time, any secondary use incompatible with the original purpose specified (e.g. marketing) should be based on the data subject's informed consent. In this respect the level of privacy guaranteed by the present RAA (cf. point II.F.6.f) is not sufficient.

Any technical mechanism to be introduced to access the data collected from the registrants must furthermore have safeguards to meet the principle of purpose limitation and avoidance of the possibility to unauthorised secondary use of the registrant's data. This demand is not met by an unrestricted, publicly available, searchable database like many WhoIs-databases currently existing. In this respect the Working Group welcomes respective proposals of WIPO in its report on the Internet Domain Name Process to make contact details of domain name holders only available for limited purposes and to take measures to discourage unauthorised secondary use e.g. for marketing purposes. The Working Group deems it necessary that filter mechanisms are developed to secure purpose limitation to be incorporated in the interfaces for accessing the database.

The Working Group further recommends that – in the absence of globally binding data protection legislation – the registries develop a uniform standard for the collection and use of personal data of domain name holders, including rules on the information of the data subjects about the purpose of the collection and of the use of their personal data and a right to access and correction of their data. Adherence to these regulations should be secured through certification procedures.

The Working Group stresses that any registrar operating within the jurisdiction of existing data protection laws and any national domain name registration procedures are subject to the existing national data protection and privacy legislation and to the control by the existing national Data Protection and Privacy Commissioners. At the same time the Working Group supports the European Commission's efforts to strengthen the protection of personal data and privacy within a functioning Internet domain name system for the benefit of all citizens and encourages the European Commission to continue its discussion with ICANN, the US Government and all other parties.

Gemeinsamer Standpunkt zu Datenschutzaspekten der Veröffentlichung personenbezogener Daten aus öffentlich zugänglichen Dokumenten im Internet

Mit der steigenden Nutzung des Internet hat die Veröffentlichung personenbezogener Daten aus öffentlich zugänglichen bzw. offiziellen Dokumenten im Internet in den letzten Jahren dramatisch zugenommen (z. B. Gerichtsentscheidungen, öffentliche Register und andere offizielle Dokumente).

Die Tatsache, dass diese Dokumente nunmehr elektronisch oder auf globaler Ebene verfügbar sind, führt zu neuen spezifischen Risiken für den Datenschutz der betroffenen Personen.

Die Arbeitsgruppe nimmt zur Kenntnis, dass die „Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten" der Datenschutzbeauftragten der Europäischen Union („Art.-29-Gruppe") diese Probleme ausführlich in ihrer Stellungnahme 3/99 betreffend die Informationen des öffentlichen Sektors und den Schutz personenbezogener Daten behandelt hat, und unterstützt die dort geäußerte Auffassung in vollem Umfang.

Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet

With the growing use of the Internet the publication of personal data contained in publicly available [official] documents on the Internet has increased dramatically over the last years (e.g. court decisions, public registers and other official documents).

The fact that these documents are now available electronically and globally causes new specific risks to the privacy of the persons concerned.

The Working Group notes that the "Working Party on the protection of individuals with regard to the processing of personal data" of Data Protection Commissioners in the European Union ("Article 29 Group") has addressed these issues extensively in their Opinion 3/99 on Public Sector information and the Protection of Personal Data and fully supports their findings.

28. Sitzung, 13. und 14. September 2000, Berlin

Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates

Vorwort

Der Europarat bereitet gegenwärtig ein „Übereinkommen über Datennetzkriminalität" vor, mit dem beabsichtigt ist, „… strafrechtliche Untersuchungen und Verfahren bezüglich der Straftaten in Verbindung mit Computersystemen und -daten wirksamer zu gestalten und um die Erfassung elektronischer Beweise bei Straftaten zu gestatten". Wichtige nichteuropäische Staaten wie die Vereinigten Staaten von Amerika, Kanada, Japan und Südafrika sind an dem Entwurfsprozess beteiligt. Der Entwurf des Übereinkommens soll bis Dezember 2000 fertig gestellt und frühestens im September 2001 zur Unterschrift aufgelegt werden. Der Entwurf selbst sieht den Beitritt weiterer Staaten auf Einladung des Ministerkomitees vor. Der Europarat hat erklärt, dass er den Konsultationsprozess mit interessierten Parteien unabhängig davon, ob es sich um öffentliche oder private Stellen handelt, vertiefen will.

Die Arbeitsgruppe erkennt an, dass eine Notwendigkeit zur internationalen Bekämpfung von Straftaten in Verbindung mit Computersystemen existiert, dass eine verbesserte internationale Kooperation in der Ära globaler Kommunikationsnetzwerke nötig ist und dass Strafverfolgungsbehörden zur Bekämpfung solcher Verbrechen angemessene Mittel benötigen. Auf der anderen Seite müssen diese Mittel mit anderen gemeinsamen Werten, z. B. dem Recht auf Datenschutz und dem Telekommunikationsgeheimnis, in Einklang gebracht werden.

Während das Europäische Übereinkommen zur Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union ausdrücklich den Schutz personenbezogener Daten regelt (Art. 23), enthält der gegenwärtige Entwurf eines Übereinkommens über Datennetzkriminalität keinen einzigen Hinweis auf Datenschutzbestimmungen. In dem Entwurf wurde auch versäumt, Verletzungen der Privatsphäre durch den einfachen Zugriff auf Computersysteme in klarer und unmissverständlicher Weise unter Strafe zu stellen.

Der Europarat verfügt über eine lange Tradition bei der Entwicklung von multilateralen Datenschutzstandards. Es scheint daher angemessen, dass in dem neuen Übereinkommen ausdrücklich auf das Übereinkommen zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) von 1981 und die Empfehlung Nr. R (95) 4 zum Schutz personenbezogener Daten auf dem Gebiet der Telekommunikationsdienste unter besonderer

Bezugnahme auf Telefondienste Bezug genommen wird. Die Arbeitsgruppe hält es für erforderlich, das Expertenkomitee des Europarates für Datenschutzfragen in den weiteren Entwurfsprozess mit einzubeziehen.

Neue Verfahren

Das Übereinkommen über Datennetzkriminalität zielt darauf ab, neue Verfahren einzuführen, um die Verfolgung von Verbrechen im Zusammenhang mit der Internetnutzung zu ermöglichen, einschließlich Maßnahmen, um Telekommunikationsdiensteanbieter zu zwingen, personenbezogene Daten (sowohl Inhalts- als auch Verbindungsdaten) von Kommunikationsvorgängen in Telekommunikations-Netzwerken zu speichern und diese nationalen und ausländischen Behörden, die mit strafrechtlichen Ermittlungen und Verfahren befasst sind, zugänglich zu machen.

Bereits in der Vergangenheit hat es eine Diskussion in verschiedenen Zusammenhängen über die Verpflichtung von Telekommunikations- und Internetdiensteanbietern gegeben, Daten über den gesamten Telekommunikations- und Internetverkehr für einen erweiterten Zeitraum zu speichern, damit diese Daten zur Verfügung stehen, wenn innerhalb dieses Zeitraums ein Verbrechen begangen wird. Die Arbeitsgruppe hält derartige Maßnahmen für unangemessen und damit inakzeptabel. Die Arbeitsgruppe unterstreicht, dass Verbindungsdaten im gleichen Ausmaß geschützt sind wie Inhaltsdaten (Art. 8 der Europäischen Menschenrechtskonvention). In dieser Hinsicht unterstützt die Arbeitsgruppe in vollem Umfang die Ergebnisse der Konferenz der Europäischen Datenschutzbeauftragten vom 6./7. April 2000 in Stockholm, bei der die Konferenz erklärt hat, dass eine solche Aufbewahrung von Verbindungsdaten durch Internetdiensteanbieter einen unangemessenen Eingriff in die den Einzelnen durch die Europäische Menschenrechtskonvention garantierten Grundrechte darstellen würde (http://www.datenschutz-berlin.de/doc/eu/konf/00_db_en.htm; vgl. auch Empfehlung 3/99 der Arbeitsgruppe nach Art. 29 zur Aufbewahrung von Verkehrsdaten durch Internetdiensteanbieter für Strafverfolgungszwecke; http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp25_en.htm). Dies gilt auch für die Speicherung von Daten, die Aufschluss über die Internetnutzung des Einzelnen geben.

Bestehende Befugnisse zur Strafverfolgung sollten nicht in einer Art ausgeweitet werden, die in die Privatsphäre eindringen, bevor die Notwendigkeit für solche Maßnahmen überzeugend dargelegt worden ist.

Die Arbeitsgruppe hat bereits in der Vergangenheit erklärt, dass jegliches Abhören von privater Kommunikation Gegenstand von angemessenen Sicherungsmaßnahmen sein muss (vgl. Gemeinsamer Standpunkt über die öffentliche Ver-

antwortung im Hinblick auf das Abhören privater Kommunikation; angenommen auf der 23. Sitzung in Hong Kong SAR, China, am 15. April 1998; http:/www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm). Existierende Bedingungen und Sicherungsmaßnahmen im nationalen Recht und dem Übereinkommen zur Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (Art. 23) müssen respektiert werden. Solche Bedingungen und Sicherungsmaßnahmen sollten wenigstens enthalten

- die vorherige richterliche Anordnung,
- die (nachträgliche) Benachrichtigung der Betroffenen,
- die Beschränkung der Nutzung,
- die Verpflichtung zur Protokollierung,
- die Überwachung und Kontrolle sowie
- eine öffentliche Rechenschaftspflicht.

Dementsprechend sollten solche Sicherungsmaßnahmen auch in den Entwurf des Übereinkommens über Datennetzkriminalität aufgenommen werden. Insbesondere die Zusammenarbeit von nationalen Behörden mit den Betreibern von öffentlichen und privaten Netzwerken sollte vorzugsweise auf eindeutige gesetzliche Verpflichtungen gegründet werden anstatt auf freiwillige Vereinbarungen, deren Einhaltung schwer zu kontrollieren ist.

Neue Straftatbestände

Gleichzeitig sieht die Konvention vor, verschiedene neue Straftatbestände einzuführen, die in den Strafgesetzen vieler Mitgliedstaaten des Europarates nicht enthalten sind.

Die Einführung neuer Straftatbestände im Strafrecht muss mit extremer Zurückhaltung behandelt werden, weil eine weite Formulierung solcher neuen Straftatbestände wie auch die Kriminalisierung von Versuch und Beihilfe zu solchen Straftaten zu einer erheblichen Absenkung des Datenschutzstandards für alle Nutzer von Telekommunikationsnetzen führen kann; dadurch würde eine enorme Menge personenbezogener Daten über die Nutzung von Telekommunikationsnetzen und des Internet entstehen, wodurch das Recht zur anonymen Nutzung dieser Dienste abgeschafft würde. Es ist vorhersehbar, dass die beabsichtigten Regelungen zur Personalisierung jeder einzelnen Handlung jedes Nutzers in dem globalen Netz führen könnten, was offensichtlich unangemessen wäre.

Hinsichtlich der Straftatbestände, die in den Artikeln 1 bis 13 behandelt werden, besonders der Kriminalisierung „unerlaubter Vorrichtungen“ (Art. 6), von „Datenveränderung“ und der „Störung des Systems“ (Art. 4 und 5), ist die Arbeitsgruppe der Ansicht, dass es zur Bekämpfung der Netzkriminalität geeigneter wäre, wenn die Vertragsstaaten des Übereinkommens sich verpflichten würden, Diensteanbieter dazu zu zwingen, bestimmte Sicherheitsmaßnahmen beim Anschluss ihrer Systeme an ein öffentliches Netzwerk zur Verbesserung des Sicherheitsstandards im Internet im Allgemeinen zu treffen als einfach neue Straftatbestände zu schaffen, die sich auf eine große Spannweite von Internetaktivitäten beziehen und sogar Aktivitäten unter Strafe stellen könnten, die zur Verbesserung der Sicherheit im Netz gedacht sind.

28th meeting, 13th and 14th September 2000, Berlin

Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe

Preface

The Council of Europe is preparing a “Convention on Cyber-crime” which intends “to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of electronic evidence of a criminal offence”. Major non-European countries, such as the United States, Canada, Japan and South Africa are participating in the drafting process. The draft Convention is expected to be finalised by December 2000 and to be open for signatures as early as September 2001. The draft itself allows for accession of any other state at the invitation of the Committee of Ministers. The Council of Europe has stated that it seeks to enhance the consultation process with interested parties, whether public or private.

The Working Group acknowledges that there is a need to fight international computer-related crime, that enhanced international co-operation is needed in the era of global communications networks and that law enforcement authorities need appropriate means for fighting such crimes. On the other hand such measures have to be balanced with other common values, e.g. the right to privacy and to telecommunications secrecy.

Whereas the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union expressly regulates the protection of personal data (Art. 23) the present draft convention on cyber-crime does not contain

any reference to privacy regulations. It fails to outlaw infringements in a clear and unambiguous way on personal privacy by the mere access to computer systems.

The Council of Europe has a longstanding tradition of developing data protection standards on a multilateral basis. It seem therefore appropriate that the new convention expressly refers to Con-vention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981 and Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services. The Working Group considers it necessary that the Committee of Experts on Data Protection is included in the further drafting process.

New Procedures

The Convention on cyber-crime intends to introduce new procedures to allow for the prosecution of crimes related to the Internet use, including measures to compel telecommunications service providers to store personal data (both content and traffic data) of communications via telecommunica-tions networks and to make these data available to the national and foreign authorities engaged in criminal investigations and proceedings.

There has been discussion in the past in different contexts on obliging telecommunications and Internet Service providers to store data on all telecommunications and Internet traffic for extended periods to have the data at hand if a crime occurs in this period. The Working Group deems such measures as disproportionate and therefore unacceptable. The Working Group underlines that traffic data are protected by the principle of confidentiality to the same extent as content data (Article 8 of the European Convention on Human Rights). In this respect the Working Group fully supports the findings of the European Data Protection Commissioners Conference at its meeting on 6/7 April 2000 in Stockholm where the Conference has stated that such retention of traffic data by Internet service providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights (http://www.datenschutz-berlin.de/doc/eu/konf/00_db_en.htm; cf. also Recommendation 3/99 of the Article 29 Working Party on the preservation of traffic data by Internet Service Providers for law enforcement purposes; http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp25_en.htm). This goes also for storing data revealing the use of the Internet by individuals.

Existing powers for tracing crimes should not be extended in a way that invades privacy until the need for such measures has been clearly demonstrated.

The Working Group has in the past stated that any Interception of Private Communications should be subject to appropriate safeguards (cf. Common Position

on Public Accountability in relation to Interception of Private Communications; adopted at the 23rd Meeting in Hong Kong SAR, China on 15 April 1998; http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm). Existing conditions and safeguards provided for under domestic law and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (Art. 23) must be respected. Such conditions and safeguards should at least include

- prior judicial authorisation,
- (subsequent) notification of individuals,
- limits on use,
- record-keeping requirements,
- monitoring and auditing as well as
- public reporting.

Accordingly such safeguards should also be incorporated in the draft Convention on cyber-crime. In particular the cooperation of national authorities with operators of public and private networks should be based on solid, legal obligations rather than on voluntary agreement that are very difficult to control.

New offences

At the same time the Convention intends that several new offences which have not been incorporated in the criminal laws of many member states of the Council of Europe may be introduced.

The introduction of new offences in the criminal law has to be handled extremely carefully, as a broad wording of such new offences as well as the penalisation of attempt and aiding and abetting such offences might lead to a considerable lowering of the privacy standard for all users of tele-communications networks by producing an enormous amount of personal identifiable data about Internet and telecommunications network usage, thus abolishing the right to anonymous use of such services. It is to be foreseen that the envisaged regulations might lead to a need to personalise every single action of every single user in the global network, which would clearly be disproportionate.

Regarding the offences that are dealt with in Articles 1–13, especially the criminalization of “Illegal devices” (Article 6), “Data Interference” and “System Inter-

ference" (Articles 4 and 5) the Working Group takes the view that obligations on the parties to the Convention to compel service providers to take certain security measures when connecting their systems to a public network in order to enhance the security standard on the Internet in general would be more suitable for fighting cyber-crime than simply creating new offences, which relate to a wide scope of internet activities and could even penalise activities which are intended to improve security of the network.

Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz („Zehn Gebote zum Schutz der Privatheit im Internet")

In seinem Eröffnungsvortrag auf der Internationalen Datenschutzkonferenz 1999 in Hong Kong hat der australische Bundesrichter Michael Kirby die Notwendigkeit neuer Prinzipien für den Datenschutz im Hinblick auf die heute gebräuchlichen Technologien betont. Diese Ausführungen waren der Ausgangspunkt für die Internationale Arbeitsgruppe, Überlegungen darüber anzustellen, welche Prinzipien essentiell für internationale (oder nationale) Übereinkommen über die spezifischen Probleme des Datenschutzes in der Telekommunikation in der Informationsgesellschaft sein könnten.

Der folgende Text ist ein erster Versuch, die gegenwärtige Diskussion zusammenzufassen und ihre Ergebnisse in Prinzipien zu überführen, die entweder in bereits bestehende Übereinkommen integriert oder als ein separates Dokument verabschiedet werden könnten. Sie enthalten Ideen, die Richter Kirby selbst in seinem Vortrag präsentiert hatte.

Zehn Gebote zum Schutz der Privatheit in der Welt des Internet

Informationelle Gewaltenteilung: Netzwerk- und Diensteanbieter dürfen keine Inhalte abhören oder beeinträchtigen, außer wenn ausdrückliche gesetzliche Regelungen es verlangen. Dort, wo Netzwerk- oder Diensteanbieter selbst Inhalte anbieten, müssen die Verantwortlichkeiten für die jeweiligen Funktionen getrennt werden.

Telekommunikationsgeheimnis: Netzwerk- oder Diensteanbieter dürfen Informationen über Inhalte oder Datenverkehr nicht weitergeben, außer für Zwecke der Telekommunikation oder wenn ausdrückliche gesetzliche Regelungen dies verlangen.

Datensparsamkeit: Die Telekommunikationsinfrastruktur muss so aufgebaut sein, dass so wenig personenbezogene Daten wie technisch möglich zum Betrieb der Netzwerke und Dienste genutzt werden.

Recht auf Anonymität: Netzwerk- und Diensteanbieter müssen jedem Nutzer die Möglichkeit zur Nutzung des Netzwerks oder den Zugang zu Diensten anonym oder unter Pseudonym anbieten. Pseudonyme, die für diese Zwecke genutzt werden, dürfen nicht aufgedeckt werden, außer wenn gesetzliche Bestimmungen dies ausdrücklich verlangen.

Virtuelles Recht, allein gelassen zu werden: Niemand darf gezwungen werden, seine personenbezogenen Daten in Verzeichnissen oder anderen Registern veröffentlichen zu lassen. Jedem Nutzer muss das Recht gegeben werden, der Erhebung seiner Daten durch eine Suchmaschine oder andere Agenten zu widersprechen. Jedem Nutzer müssen das Recht und die technische Möglichkeit gegeben werden, das Eindringen externer Programme in seine eigenen Endgeräte zu verhindern.

Recht auf Sicherheit: Jedem Nutzer müssen das Recht und die technische Möglichkeit eingeräumt werden, seine Inhalte vertraulich unter Nutzung geeigneter Methoden wie Verschlüsselung zu übertragen.

Beschränkung zweckfremder Nutzung: Verbindungsdaten dürfen ohne die ausdrückliche Einwilligung des Nutzers nicht für andere Zwecke außerhalb der Notwendigkeit zum Betreiben des Netzwerkes oder Dienstes genutzt werden.

Transparenz: Netzwerk- und Diensteanbieter müssen alle notwendigen Erklärungen, die zum Verständnis der Struktur des Netzwerks oder Dienstes, der diesbezüglichen Verantwortlichkeiten, des Umfangs der verarbeiteten personenbezogenen Daten und der geplanten Übermittlungen notwendig sind, in angemessener Weise veröffentlichen.

Recht auf Auskunft: Jedem Nutzer muss das individuelle Recht gewährt werden, über alle personenbezogenen Daten, die über ihn oder sie zum Betrieb des Netzwerks oder Dienstes online verarbeitet werden, Auskunft zu erhalten.

Internationale Konfliktlösung: Angesichts der internationalen Aspekte aller Netzwerk- und Diensteaktivitäten muss jedem Nutzer das Recht gewährt werden, sich an eine Einrichtung mit grenzüberschreitenden Befugnissen zur Untersuchung und Durchsetzung zu wenden, wo nationale Gesetzgebung zur Garantie seiner Rechte nicht ausreichend ist.

Die Arbeitsgruppe ruft internationale Organisationen und öffentliche und private Einrichtungen auf, diese Prinzipien in ihre Regulierungsrahmen und Selbstverpflichtungen aufzunehmen.

Ten Commandments to protect Privacy in the Internet World Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements

In his keynote speech to the 1999 International Conference of Data Protection and Privacy Commissioners in Hong Kong Australian High Court Justice Michael Kirby, stressed the need for new privacy principles apt to contemporary technology. This remark was an incentive for the International Working Group to consider which principles could be essential for international (or national) agreements regarding the specific problems of telecommunications privacy in the information society.

The following text is a first attempt to resume the actual discussion and transform their results into principles which could be either integrated in existing agreements or be adopted as a separate document. They encompass ideas Justice Kirby presented himself in his speech.

Ten Commandments to protect Privacy in the Internet World

Informational Separation of Powers: Network and Service Providers must not intercept or interfere with any contents except where explicit law requires it. Insofar as Network or Service Providers provide contents themselves, responsibilities for the respective functions have to be separated.

Telecommunications Secrecy: Network and Service Providers must not disclose any information on contents or data traffic except for the purposes of telecommunications or where explicit law requires it.

Data Austerity: Telecommunications infrastructure has to be designed in a way that as few personal data are used to run the networks and services as technically possible.

Right to Anonymity: Network and Service Providers have to offer to any user the option to use the network or to access the services anonymously or using a pseudonym. Pseudonyms which are used for this reason must not be revealed except where explicit law requires it.

Virtual Right to be Alone: Nobody must be forced to let his or her personal data be published in directories or other indices. Every user has to be given the right to object to his or her data being collected by a search engine or other agents. Every user has to be given the right and the technical means to prevent the intrusion of external software into his own devices.

Right to Security: Every user has to be given the right and the technical means to communicate his contents confidentially by using suitable methods such as encryption.

Restriction on Secondary Use: Traffic data must not be used for other purposes than those which are necessary to run the networks or services without explicit consent of the user.

Transparency: Network and Service Providers have to publish in a reasonable way all necessary explanations that is necessary for users to recognise the structure of the network or service, the respective responsibilities, the amount of personal data being processed, and the planned disclosure.

Access to personal data: Every user has to be given the individual right to be informed on all personal data which are processed about him or her to run the network or service on-line.

International Complaints Resolution: Facing the international aspects of all network and service activities every user has to be given the right to complain to an authority with transborder powers of investigation and enforcement if national legislation is not sufficient to guarantee his or her rights.

The Working Group calls upon international organisations and public and private agencies to incorporate these principles into their policies and regulatory framework.

2001

29. Sitzung, 15. und 16. Februar 2001, Bangalore, Indien

Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten

– überarbeitet und ergänzt auf der 36. Sitzung am 18./19. November 2004 in Berlin –

Aufenthaltsinformationen wurden in mobilen Kommunikationsdiensten von Anfang an verarbeitet. Solange diese Informationen nur zum Aufbau und zur Aufrechterhaltung einer Verbindung zu dem mobilen Endgerät generiert und genutzt wurden, verfügten nur die Anbieter von Telekommunikationsnetzen, die

in den meisten Ländern sehr strikt auf die Wahrung des Fernmeldegeheimnisses verpflichtet sind, über Aufenthaltsinformationen. Die Genauigkeit der Ortung richtete sich nach der Größe der betreffenden Funkzelle in den zellularen Netzwerken.

Teilweise veranlasst durch gesetzliche Verpflichtungen, präzisere Informationen über den Aufenthaltsort eines mobilen Endgerätes für Rettungsdienste verfügbar zu machen, haben die Betreiber von Netzwerken damit begonnen, die technische Infrastruktur ihrer Netzwerke zu verändern, um diese Verpflichtungen zu erfüllen. Dies bedeutet, dass in naher Zukunft wesentlich genauere Informationen über den Aufenthaltsort eines jeden mobilen Endgerätes verfügbar sein werden. Endgerätehersteller geben an, dass selbst heute eine Präzision von bis zu fünf Metern technisch möglich ist, wenn GPS-unterstützte Systeme benutzt werden. Gleichzeitig ist abzusehen, dass die Entwicklung des mobilen elektronischen Geschäftsverkehrs zur Schaffung einer Vielzahl neuer Dienste führen wird, die auf der Kenntnis des präzisen Aufenthaltsortes des Nutzers basieren. Diese Dienste werden aller Wahrscheinlichkeit nach nicht nur von Telekommunikationsdiensteanbietern, sondern auch von Dritten angeboten werden, die nicht an die gesetzlichen Beschränkungen des Fernmeldegeheimnisses gebunden sind.

Die verbesserte Genauigkeit von Aufenthaltsinformationen und ihrer Verfügbarkeit nicht nur für die Betreiber mobiler Telekommunikationsnetzwerke kann neue, bisher nicht da gewesene Risiken für den Datenschutz von Nutzern mobiler Endgeräte in Telekommunikationsnetzwerken zur Folge haben. Die Arbeitsgruppe hält es dafür für erforderlich, dass die Technologie zur Ortung mobiler Endgeräte in einer Weise entwickelt wird, die die Privatsphäre so wenig wie möglich beeinträchtigt.

Hinsichtlich des Angebots von Mehrwertdiensten sollten die folgenden Prinzipien beachtet werden:

1. Der Entwurf und die Auswahl technischer Einrichtungen solcher Dienste sollten an dem Ziel orientiert sein, entweder überhaupt keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

2. Präzise Aufenthaltsinformation sollte nicht als ein Standardleistungsmerkmal eines Dienstes generiert werden, sondern nur „nach Bedarf“, wenn dies notwendig ist, um einen bestimmten Dienst zu erbringen, der an den Aufenthaltsort des Nutzers geknüpft ist.

3. Der Nutzer muss die volle Kontrolle darüber behalten, ob präzise Aufenthaltsinformationen im Netzwerk entstehen. In dieser Hinsicht scheinen Endgerätebasierte Lösungen, bei denen die Entstehung präziser Aufenthaltsinformation durch das mobile Endgerät initiiert wird, ein höheres Maß an Datenschutz zu

bieten als Netzwerk-basierte Lösungen, bei denen Aufenthaltsinformationen als ein Standard-Leistungsmerkmal generiert und die Kontrolle des Nutzers sich darauf beschränkt, in welchem Umfang diese Informationen an Dritte übermittelt werden. In jedem Fall sollte der Mobilfunkteilnehmer immer in der Lage sein, sowohl die Inanspruchnahme jedes standortbezogenen Dienstes als auch spezieller standortbezogener Dienste zu kontrollieren. Der Anbieter sollte dem Teilnehmer die Möglichkeit einräumen, bei Abschluss des Teilnehmervertrags in die Nutzungsmöglichkeit jedes standortbezogenen Dienstes einzuwilligen. Der Teilnehmer darf bereits zu diesem Zeitpunkt oder später seine Zustimmung geben und darf die Inanspruchnahme sämtlicher Dienste jederzeit ablehnen. In Fällen, in denen der Mobilfunkteilnehmer eingewilligt hat, sollte der Mobilfunknutzer, der nicht mit dem Teilnehmer identisch ist, die Möglichkeit haben den Dienst zu akzeptieren oder abzulehnen.

4. Der Telekommunikationsdiensteanbieter darf nur in den Fällen Informationen an Dritte liefern, in denen der Mobilfunkteilnehmer zu der anderweitigen Nutzung der Aufenthaltsinformationen seine informierte Einwilligung erteilt hat. Nutzer sollten die Möglichkeit haben, die präzise Aufenthaltsbestimmung jederzeit abschalten zu können, ohne dafür die Verbindung ihres Endgerätes zum Netzwerk trennen zu müssen. Nutzer und Teilnehmer sollten auch die Möglichkeit haben, Aufenthaltsinformationen mit einem selbstgewählten Grad von Genauigkeit zu offenbaren (z. B. auf der Ebene eines einzelnen Gebäudes, einer Straße, einer Stadt oder eines Bundesstaates).

5. Aufenthaltsinformation sollte Anbietern von Mehrwertdiensten nur zugänglich gemacht werden, wenn der Nutzer seine informierte Einwilligung zu einer solchen Offenlegung erteilt hat. Die Einwilligung kann auf eine einzelne Transaktion oder bestimmte Anbieter von Mehrwertdiensten beschränkt sein. Der Nutzer muss in der Lage sein, auf Daten über seine Präferenzen zuzugreifen, diese zu berichtigen und zu löschen, unabhängig davon, ob diese auf dem mobilen Endgerät oder innerhalb des Netzwerkes gespeichert sind.

6. Die Erstellung von Bewegungsprofilen durch Anbieter von Telekommunikationsdiensten und Anbieter von Mehrwertdiensten sollte durch Gesetz strikt verboten werden, außer wenn dies für die Erbringung eines bestimmten Dienstes notwendig ist und der Nutzer hierzu zweifelsfrei seine informierte Einwilligung gegeben hat.

7. Daten über den Aufenthaltsort stellen eine hoch sensible Kategorie von Informationen dar. Der Zugriff auf solche Informationen sowie deren Übermittlung und Nutzung sollten Gegenstand der gleichen oder gleichartiger Kontrollen sein wie für Inhaltsdaten, die durch das Fernmeldegeheimnis geschützt werden. Die Arbeitsgruppe weist auf ihren Gemeinsamen Standpunkt über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunika-

tion hin (Hong Kong, 15. April 1998; http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_de.htm).

8. Wo immer dies möglich ist, sollten Betreiber von Mobilfunknetzen Aufenthaltsinformationen nicht zusammen mit personenbezogenen Informationen über den Nutzer an Anbieter von Mehrwertdiensten weiterleiten. Stattdessen sollten pseudonymisierte Informationen genutzt werden. Personenbezogene Informationen (z. B. die Kennung eines mobilen Endgerätes) sollten Anbietern von Mehrwertdiensten nur zugänglich gemacht werden, wenn der Nutzer seine informierte Einwilligung gegeben hat. Jegliche Aufenthaltsinformation sollte vom Anbieter gelöscht werden, sobald sie für die Erbringung des Dienstes nicht länger erforderlich ist.

9. Ein Anbieter darf die Nutzung eines Dienstes oder die Bedingungen für die Nutzung eines Dienstes nicht von der Einwilligung des Nutzers in die Verarbeitung personenbezogener Aufenthaltsinformationen abhängig machen, wenn diese Daten für die Erbringung des Dienstes nicht erforderlich sind.

29th meeting, 15th and 16th February 2001, Bangalore, India

Common Position on Privacy and location information in mobile communications services

– revised at the 36th meeting on 18–19 November 2004 in Berlin –

Location information has been processed in mobile communications networks from the very beginning. As long as this information was only generated and used for establishing and maintaining a connection to the mobile device, location information resided only with the operators of telecommunications networks, which are in most countries bound very strictly by telecommunications secrecy legislation. The precision of the location information was dependent upon the size of the respective cells in the cellular networks.

Partly driven by legal obligations to make more precise location information about mobile devices available for use by emergency services, network operators have started to modify the technical infrastructure of their networks to conform with these obligations. This means that much more precise information about the location of any mobile device will become available in the near future. Equipment manufacturers claim that even today a precision of up to 5 meters is technically feasible when using GPS-assisted systems. At the same time it is envisaged that the developing mobile electronic commerce will lead to the creation of a wealth of new services based on knowledge about the more precise location of the user.

However, such services will most likely not only be provided by telecoms operators, but also by third parties which may not be legally bound by the restrictions of telecommunications secrecy.

The enhanced precision of location information and its availability to parties other than the operators of mobile telecommunications networks create unprecedented threats to the privacy of the users of mobile devices linked to telecommunications networks. Accordingly, the Working Group recommends that the technology for locating mobile devices should be designed to be minimally invasive to privacy.

The following principles should be observed, with respect to the provisions of value added services:

1. The design and selection of technical solutions to be used for such services must be oriented to the goal of collecting, processing and using either no personal data at all or a minimal amount of personal data.

2. Precise location information should not normally be generated as a standard feature of the service, but only "on demand" where it is needed to provide a certain service that requires knowledge of the location of the user's device.

3. The user must remain in full control of the generation of precise location information within the network. In this respect, handset-based solutions where the creation of precise location information is initiated by the mobile device appear to offer a better degree of privacy than network-based solutions where location information may be generated as a standard feature and the user control is limited to the extent to which it may be communicated to third parties. However, the mobile subscriber should always be able to control both the possibility of using any location services or specific location services. The provider should give the subscriber the opportunity to opt-in to the possibility of the use of any location services when presenting the subscriber contract. The subscriber may opt-in at this point or at any future time and may opt-out of all location services at any time. Where the mobile subscriber may have opted in, the mobile user should be free to give consent or to opt out of the service.

4. The telecommunication provider may only deliver location information to a third party in cases where the mobile subscriber has given his informed consent to the operator on the alternative use of location information.* Users

* Cf. Art. 6 and 9 Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

should be able to disable the precise determination of their location at any time without disconnecting their device from the network. Users or mobile subscribers should also be able to enable the disclosure their location information at a chosen level of precision (e.g. building, street, city or state level).

5. Location information should only be made available to providers of value added services where the user has given his informed consent to such disclosure. Consent may be restricted to a single transaction or to certain providers of value added services. The user must be able to access, correct and delete his or her preference data whether such data stored on the mobile device or within the network.

6. The creation of movement profiles by telecommunications service providers and providers of value added services should be strictly forbidden by law other than where necessary for the provision of a certain service and conditional on the user's informed, unambiguous consent.

7. Location information is a highly sensitive category of information. Access, use and disclosure of such information should be subject to the same or similar controls as for content data that are protected by telecommunications secrecy. The Working Group refers to its Common Position on Public Accountability in relation to Interception of Private Communications (Hong Kong, 15.04.1998; http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm).

8. Wherever possible, mobile network operators should not communicate location information together with personally identifiable information about the user to providers of value added services. Instead, pseudonymous information should be used. Personally identifiable information (e.g. the ID of the mobile device) should only be made available to providers of value added services with the user's informed consent. Any location information should be deleted by the service provider when no longer necessary for the provision of that service.

9. A provider must not make the rendering of a service or the terms of the service conditional upon the consent of the user to the effect that his or her personal localisation data may be processed where such data are not necessary for the provision of the service.

30. Sitzung, 28. August 2001, Berlin

Arbeitspapier zu Datenschutz und internetgestützter Stimmabgabe bei Wahlen zu Parlamenten und anderen staatlichen Einrichtungen[1]

Moderne Kommunikationstechnologien, insbesondere das Internet, können möglicherweise einen zusätzlichen Weg zur Vorbereitung und Erleichterung der Teilnahme an Wahlen auf örtlicher, staatlicher und weltweiter Ebene eröffnen. „Online Voting" (Stimmabgabe online), „Electronic Voting" (Elektronische Stimmabgabe) und „e-democracy" (Elektronische Demokratie) sind Schlagwörter in der jüngsten öffentlichen Diskussion. In einer Reihe von Ländern wird gegenwärtig der Rechtsrahmen verändert, um elektronische Abstimmungsmethoden zuzulassen. Universitäten und andere Körperschaften haben interne internetgestützte Wahlen für Vertretungskörperschaften von Studenten durchgeführt.

Zwei Formen der elektronischen Abstimmung können unterschieden werden:

- elektronische Abstimmung mit zertifizierter Hard- und Software in offiziellen Abstimmungslokalen („Geschlossene" oder „Ende-zu-Ende-Systeme");

- elektronische Abstimmung von jedem Eingabegerät (z. B. private PC's, Handies) mit nichtzertifizierter Software („Offene Systeme").

Die zweite Variante führt zu dem allgemeinen Problem der Briefwahl, da das Wahlgeheimnis nicht in der gleichen Weise in einer Privatwohnung oder am Arbeitsplatz gesichert ist wie in einer Abstimmungskabine.

Jede Technologie, die in diesem Zusammenhang eingesetzt wird, muss grundlegende verfassungsrechtliche Bedingungen für ein demokratisches Wahlverfahren erfüllen. Es ist allgemein akzeptiert, dass Wahlen zu Parlamenten und anderen staatlichen Einrichtungen frei, gleich und geheim sein müssen. Gleichzeitig muss das Wahlverfahren transparent und für die Öffentlichkeit überprüfbar sein.

Im Fall von bindenden Wahlen zu Parlamenten und anderen repräsentativen Körperschaften ist das Erfordernis des Wahlgeheimnisses entscheidend. Gleichzeitig muss das Wahlgeheimnis mit der Transparenz und Überprüfbarkeit des gesamten Wahlverfahrens in Einklang gebracht werden. Die Erfahrung der Überwachung und Manipulation von Wahlen in nichtdemokratischen Staaten hat unterstrichen, dass die Vertrauenswürdigkeit jedes politischen Systems hier auf dem Spiel steht. Während papiergestützte Wahlen transparent sind, trifft dies für elektronische

[1] Das Arbeitspapier beschränkt sich auf Wahlen zu repräsentativen Körperschaften und öffentlichen Ämtern. Der Begriff „staatlich" umfasst alle (also legislative, exekutive und justizielle) Zweige der Staatsorganisation.

Wahlverfahren nicht in gleicher Weise zu. Elektronische Abstimmungsverfahren können sogar sicherer sein als konventionelle Abstimmungsmethoden. Die Wahl muss aber nicht nur sicher sein, sondern ihre Sicherheit muss auch sichtbar werden. Verschlüsselungsmethoden (z. B. blinde Signaturen) und die informationelle Trennung von Befugnissen und Funktionen (informationelle Gewaltenteilung) zwischen Rechnern, die die Wahlberechtigung überprüfen und die Stimmen sammeln und zählen, werden gegenwärtig diskutiert. Sie sind äußerst komplex, müssen aber zugleich einen Ausgleich für den Mangel an Transparenz schaffen. Diese Vorschläge werden sorgfältig zu prüfen und öffentlich zu diskutieren sein. Da das Vertrauen der Wählerschaft für den demokratischen Prozess entscheidend ist, sollte hier mit erheblicher Vorsicht vorgegangen werden. Die US-Präsidentschaftswahlen 2000 haben die bei der Abstimmung eingesetzte Technik zum Gegenstand einer intensiven öffentlichen Auseinandersetzung gemacht. Öffentlicher Unmut kann entstehen, wenn die bei Abstimmungen eingesetzte Technologie nicht vertrauenswürdig ist oder den Willen der Öffentlichkeit bei Abstimmungs-, Zähl- und Prüfverfahren zu vereiteln scheint.

Die Arbeitsgruppe macht deshalb die folgenden Empfehlungen:

1. Die komplizierten technischen Fragen bezüglich der Verlässlichkeit einschl. der Sicherheit und Verfügbarkeit von elektronischen Wahlsystemen (Schutz gegen unbefugten Zugriff und Überflutungsangriffe) sollten beantwortet werden, bevor ein derartiges System bei Wahlen zu gesetzgebenden oder anderen staatlichen Körperschaften auf irgendeiner Ebene eingesetzt wird; diese Systeme sollten einer gründlichen Risikoanalyse und Testverfahren unterzogen werden[2].

2. Authentifizierungsverfahren für Wähler bei elektronischen Abstimmungen, die vor der Stimmabgabe eingesetzt werden, um das Wahlrecht zu prüfen, eine mehrfache Stimmabgabe zu unterbinden und gleichzeitig das Wahlgeheimnis zu sichern, sollten nicht weniger sicher sein als die Verfahren, die bei papiergestützten Abstimmungen angewandt werden.

3. Während das System einerseits den Wähler warnen sollte, wenn die Stimme nicht registriert oder korrekt übermittelt worden ist, muss andererseits eine quittungsfreie Stimmabgabe sichergestellt sein, um die Gefahr der Beeinflussung zukünftiger Wähler und der Erpressung solcher Personen, die ihre Stimme abgegeben haben, zu verringern. Eine Zwischenspeicherung oder elektronische Registrierung von individuellen abgegebenen Stimmen sollte nach ihrer Zählung nicht zugelassen werden.

[2] Neuere Forschungsergebnisse in den Vereinigten Staaten deuten darauf hin, dass es zumindest 10 Jahre dauern kann, bevor dieses Ziel erreicht ist; vgl. den Bericht des California Institute of Technology/Massachusetts Institute of Technology, Voting Technology Project, Voting – What Is – What Could Be, July 2001, http://www.vote.caltech.edu/Reports/index.html

4. Die gesamte Hard- und Software einschl. des Quellcodes muss dokumentiert und einer Prüfung zugänglich gemacht werden.

5. Vertrauenswürdige Zertifizierungsverfahren für Hard- und Software müssen eingesetzt werden.

30th meeting, 28th August 2001, Berlin

Working Paper on Data Protection and Online Voting in Parliamentary and other Governmental Elections[1]

Modern communications technology, in particular the Internet, may have the potential to be used as an additional way of preparing or facilitating participation in elections on local, state or worldwide levels. "Online voting", "electronic voting" and "e-democracy" are keywords in recent public discussions. In a number of countries the legal framework is being changed to allow for online voting. Universities and other bodies have held internal online elections for representative bodies of students.

Two forms of online voting can be distinguished:

- online voting with certified hard- and software at official polling stations ("closed" or "end-to-end"-systems);

- online voting from any input device (e.g. home PCs, mobile phones) with uncertified software ("open systems").

The second option leads to a general problem of absentee voting since ballot secrecy is not ensured on the same level at one's home or place of employment as in a polling booth.

Any technology used in this context has to meet the basic constitutional requirements for a democratic voting procedure. It is generally accepted that parliamentary and other governmental elections have to be free, equal and secret. At the same time the election procedure has to be transparent and subject to public scrutiny.

[1] The scope of this paper is restricted to elections for representative political bodies and public offices. The term "Governmental" includes all (i.e. the legislative, executive and judicial) branches of government.

In the case of binding elections for parliaments and other representative political bodies the requirement of ballot secrecy is crucial. At the same time ballot secrecy will have to be reconciled with transparency and auditability of the entire voting procedure. The experience of surveillance and vote-rigging in non-democratic societies has underlined that the trustworthiness of any political system is at stake here. Whereas paper-ballot elections are transparent online voting procedures are not transparent to same extent. Online voting may be even more secure than conventional voting methods. However, voting not only has to be secure, it has to be seen to be secure. Cryptographic methods (e.g. blind signatures) and the informational separation of powers and functions (separation of privilege). between severs which check voter registration and which collect and count votes are under discussion. They are highly complex but at the same time they will have to compensate for the lack of transparency. These proposals have to be scrutinised carefully and discussed in public. Since voter confidence is essential for the democratic process considerable caution is appropriate. The US Presidential Election 2000 put voting technology at the centre of intense public controversy. Public unease can arise if voting technology is not trusted or is perceived to frustrate the public's will in the voting, counting or checking processes.

The Working Group therefore makes the following recommendations:

1. The complex technical questions with regard to dependability including security and availability of online voting systems (protection against unauthorized access and "denial of service"-attacks) should be answered before any such system is used at parliamentary and other governmental elections on any level; these systems should be subject to a thorough risk analysis and testing[2].

2. Authentication procedures for voters in electronic ballots which are used before casting the vote in order to ascertain the right to vote, to prevent votes being cast more than once and at the same time to ensure ballot secrecy, should be no less secure than the procedures used in paper ballots.

3. While the system should warn the voter if the vote has not been registered or transmitted correctly, receipt-free vote casting must be ensured in order to diminish the risk of influencing prospective voters or victimising those who have voted. No caching or electronic recording of the individual votes cast should be allowed after they have been counted.

4. The entire hard- and software including the source-code has to be documented and open to scrutiny.

[2] Recent research in the U.S. suggests that it might take at least ten years before this goal is achieved; cf. the Report of the California Institute of Technology / Massachusetts Institute of Technology, Voting Technology Project, Voting – What Is – What Could Be, July 2001, <http://www.vote.caltech.edu/Reports/index.html>

5. Trusted certification procedures for hard- and software have to be implemented.

Arbeitspapier zu Datenschutzaspekten digitaler Zertifikate und public-key-Infrastrukturen

Instanzen, die miteinander kommunizieren – ob mit Hilfe elektronischer oder anderer Mittel – können alle Arten von Anforderungen an die Sicherheit und Verlässlichkeit des Informationsaustausches haben. Wichtige Aspekte beinhalten die Identifikation, Authentifizierung, Autorisierung, Vertraulichkeit, Integrität und Nichtabstreitbarkeit.

Kryptographie ist eine beinahe unverzichtbare Technik, um diese Eigenschaften in einem offenen, elektronischen Umfeld zu garantieren. Eine Technik, deren Popularität rapide zunimmt, ist die *public-key-Kryptographie.* Diese Technik verwendet zwei verschiedene Schlüssel, von denen einer benutzt wird, um Nachrichten zu verschlüsseln, und der andere, um sie zu entschlüsseln. Einer dieser beiden Schlüssel, der private Schlüssel, muss von seinem Inhaber geheim gehalten werden, der andere wird von ihm öffentlich zur Verfügung gestellt. Public-key-Kryptographie kann auf zwei Arten angewendet werden. Wenn der Schlüssel zur Verschlüsselung veröffentlicht wird, kann jedermann diesen Schlüssel benutzen, um eine verschlüsselte Nachricht zu erzeugen, die nur der Besitzer des dazugehörigen privaten Schlüssels entschlüsseln kann. Wenn auf der anderen Seite der Entschlüsselungsschlüssel veröffentlicht wird, kann er benutzt werden, um die Quelle einer verschlüsselten Nachricht zu authentifizieren: Nur der Besitzer des korrespondierenden privaten Schlüssels kann die Nachricht verschlüsselt haben. Diese letztgenannte Anwendung ist als *digitale Signatur* bekannt.

Die Nutzung von public-key-Kryptographie erfordert, dass der Schlüssel in verlässlicher Weise mit der Identität oder anderen Attributen des Schlüsselinhabers verbunden wird. Die Infrastruktur, die benötigt wird, um dies zu ermöglichen, wird als *public-key-Infrastruktur* (PKI) bezeichnet. Ein *vertrauenswürdiger Dritter (trusted third party,* TTP) garantiert diese Verbindung in einer PKI[1]. Die TTP erreicht dies, indem sie selbst eine digitale Signatur benutzt. Ein *digitales Zertifikat* ist jegliches digital signierte Dokument. Digitale Zertifikate werden üblicherweise von einer TTP herausgegeben und von ihr digital signiert; sie verbinden dann einen öffentlichen Schlüssel mit Attributen des Schlüsselinhabers.

[1] Die Europäische Richtlinie 99/93/EG hat die Bezeichnung „Zertifikatsdiensteanbieter" für TTPs eingeführt, die alle oder einige der Dienste anbieten, die notwendig sind, um diese Garantie herzustellen.

Wenigstens drei wesentliche Datenschutzaspekte sind mit der Nutzung von öffentlichen public-key-Infrastrukturen verbunden:

A. Bezeichnung und Identität, Pseudonymität, Anonymität;

B. Verbreitung von PKI-Information;

C. rechtmäßiger Zugang.

A. Bezeichnung und Identität, Pseudonymität, Anonymität

Normalerweise ist wünschenswert, dass die Identität eines digital Unterzeichnenden bekannt ist. Dies bedeutet allerdings nicht, dass diese Identität auch in dem Zertifikat enthalten sein muss. Es ist oftmals ausreichend, dass sie, wenn notwendig, festgestellt werden kann, z. B. im Fall von Betrug. Da der Nutzer eines pseudonymen Zertifikats eine offensichtliche Absicht hat, seine Identität zu verbergen, muss genau festgelegt werden, welche Umstände hinreichende Gründe darstellen, diese Daten trotzdem an Dritte weiterzugeben.

Modelle für „PET“[2]-Zertifikate, die durch Nutzung von Pseudonymen unter anderem die Privatsphäre schützen, verdienen mehr Aufmerksamkeit, als sie bisher erhalten haben. Dies würde dazu beitragen, das Potential der public-key-Kryptographie als eine wichtige datenschutzfreundliche Technologie zu verwirklichen.

Traditionelle identifizierende Daten wie Namen, Adresse und Wohnort sind eine nicht hinreichende Basis, personenbezogene Daten verlässlich zu verbinden. Solche Verbindungen können der Qualität der Daten dienen, sie können allerdings auch große Risiken für den Datenschutz mit sich bringen. Aus diesem Grunde ist die Einführung von national oder sogar global eindeutiger Identifikatoren nicht wünschenswert. Sektorale oder Ketten-basierte Identifikatoren können eine alternative Lösung darstellen. Öffentliche Schlüssel oder – noch gefährlicher – biometrische Merkmale dürfen nicht zu alternativen, eindeutigen Identifikatoren werden.

B. Verbreitung von PKI-Informationen

Innerhalb einer PKI ist es notwendig, verschiedene Arten von Information zu verbreiten. Die bedeutendsten sind Zertifikat-Informationen und Widerrufs-Informationen.

[2] PET = privacy-enhancing technology (datenschutzfreundliche Technologie).

Die populärste Art, Zertifikate zu verbreiten, ist ein Verzeichnis. Dies sollte nur mit der Erlaubnis des Inhabers des Zertifikats erfolgen, dem auch eine tatsächliche Alternative zur Verfügung gestellt werden muss. Die Erlaubnis muss freiwillig gegeben werden und auf korrekten, klaren und vollständigen Informationen basieren. Wenn Zertifikate im großen Umfang öffentlich zugänglich sind, eröffnet dies alle Arten von Möglichkeiten zur Erstellung detaillierter Profile. Daher verdient die private Verbreitung als eine Alternative ernsthafte Aufmerksamkeit, bei der der Inhaber des Zertifikats selbst für die Lieferung des Zertifikats an eine verifizierende Instanz verantwortlich ist.

Widerrufs-Information, die verbreitet wird, darf nicht mehr Daten als notwendig enthalten, z. B. nur eine Seriennummer anstatt des gesamten widerrufenen Zertifikats.

PKI-Information wird für einen bestimmten Zweck verbreitet. Die weitere Verarbeitung dieser Information muss mit diesem Zweck vereinbar sein. Dies gilt auch für die Verbreitung durch ein Verzeichnis. Dieses muss entsprechend aufgebaut sein.

C. Rechtmäßiger Zugang

Verschiedene Parteien können Zugriff auf die bei den TTPs vorhandenen Daten verlangen. Die gewünschte Information kann die Identität des Inhabers eines pseudonymen Zertifikats sein, der Schlüssel zur Entschlüsselung verschlüsselter Nachrichten oder Dateien oder die Nachrichten oder Dateien selbst. Strafverfolgungsbehörden und Geheimdienste haben üblicherweise verschiedene spezifische gesetzliche Befugnisse in diesem Bereich. Andere Parteien haben normalerweise rechtmäßigen Zugriff auf der Basis eines generelleren Rechts auf bestimmte Informationen. Die Arbeitsgruppe spricht sich für eine Herangehensweise aus, die einen Ausgleich zwischen den Prüfungsbedürfnissen von Regierungen und dem Recht auf Datenschutz ihrer Bürger schafft. Das Vertrauen des Benutzers ist eine *conditio sine qua non* für TTPs. Es ist daher in den Kreisen der TTP üblich, den Prinzipien des Datenschutzes das Wort zu reden. Unglücklicherweise gehen diese Äußerungen selten über generelle Bemerkungen wie „… natürlich halten TTPs die Datenschutzgesetze ein…“ hinaus. Die Garantie eines angemessenen Schutzes personenbezogener Daten verlangt allerdings, dass dieser Aspekt zum frühestmöglichen Zeitpunkt bereits in der Designphase von Technologien und Infrastrukturen in Betracht gezogen wird. Wenn dies getan wird, können TTP-Dienste im Allgemeinen und digitale Zertifikate im Besonderen einen bedeutenden Beitrag zum Datenschutz bei elektronischen Transaktionen und der elektronischen Kommunikation leisten.

Die Arbeitsgruppe gibt daher die folgenden Empfehlungen:

1. Pseudonyme (oder sogar anonyme) Zertifikate sind identifizierenden Zertifikaten in allen Fällen vorzuziehen, in denen die Identifikation des Zertifikatinhabers im Hinblick auf den spezifischen Zweck, für den das Zertifikat benutzt wird, nicht erforderlich ist. TTPs sollten aktiv zur Entwicklung von Technologien und Infrastrukturen beitragen, die die größtmögliche Nutzung solcher Zertifikate, ob im Rahmen des X.509-Standards oder nicht, erlauben. In Situationen, in denen die Nutzung identifizierender Zertifikate nicht verhindert werden kann, sollten solche Zertifikate anonym oder pseudonym genutzt werden, wenn immer dies möglich ist.

2. Die Nutzung von nationalen oder sogar globalen eindeutigen Identifikatoren sollte im Hinblick auf die ernsten Risiken für den Datenschutz vermieden werden. Es gibt andere Möglichkeiten wie den Einsatz von sektoralen oder Ketten-basierten Nummern. Ein darauf basierender Informationsaustausch sollte mit hinreichenden Sicherungsmaßnahmen begleitet werden. PKIs sollten so konstruiert sein – z. B. durch das Angebot multipler, kurzlebiger und/oder Rollen-basierter Zertifikate –, dass Zertifikatsnummern, öffentliche Schlüssel oder biometrische Merkmale nicht zu alternativen, eindeutigen Indikatoren werden.

3. Verzeichnisse öffentlicher Zertifikate sollten – soweit dies möglich ist – so konstruiert werden, dass sie nur solche Anfragen zulassen, die im Hinblick auf den Zweck des Verzeichnisses erforderlich sind. Die Betroffenen sollten die Möglichkeit erhalten, nicht in einem solchen Verzeichnis aufgeführt zu werden; d. h., die private Verteilung von Zertifikaten muss dem Inhaber des Zertifikats als eine wirkliche Alternative zur Verfügung gestellt werden.

4. TTPs dürfen die zu einem Pseudonym gehörige Identität nur im Falle einer gesetzlichen Verpflichtung, die auf einer dringenden sozialen Notwendigkeit basiert, oder mit der ausdrücklichen Einwilligung des Inhabers des Zertifikats aufdecken.

5. Die Befugnisse von Strafverfolgungseinrichtungen und Geheimdiensten im Hinblick auf den rechtmäßigen Zugang sollten mit dem Schutz der Grundrechte und -freiheiten und insbesondere personenbezogener Daten in Einklang gebracht werden.

Working Paper on Data protection aspects of digital certificates and public-key infrastructures

Parties that communicate with each other-whether by electronic means or otherwise-may have all sorts of requirements for the security and reliability of their exchange of information. Important issues include identification, authentication, authorization, confidentiality, integrity and non-repudiation.

Cryptography is an almost inevitable technique for guaranteeing these characteristics in an open electronic environment. A technique that is rapidly gaining in popularity is *public-key cryptography*. This technique uses two different keys, one of which is used for encrypting messages and the other for decrypting them. One of these two keys, the private key, the owner must keep a secret, the other one he makes public. Public-key cryptography can be employed in two ways. When the encryption key is made public, everyone can use this key to create an encrypted message that only the owner of the corresponding private key can decrypt. When on the other hand the decryption key is made public, it can serve to authenticate the source of an encrypted message: only the owner of the corresponding private key could have encrypted the message. This last application is known as a *digital signature*.

The use of public-key cryptography requires that the key be linked in a reliable way to the identity or other attributes of the key holder. The infrastructure required to facilitate this is known as a *public-key infrastructure* (PKI). A *trusted third party* (TTP) guarantees this link in a PKI[1]. The TTP does so by using a digital signature itself. A *digital certificate* is any digitally signed document. Digital certificates are most commonly issued and digitally signed by a TTP, and then link a public key to attributes of the key holder.

At least three major data protection issues are connected with the use of public PKI's:

A. naming and identity, pseudonimity, anonymity;

B. dissemination of PKI information;

C. lawful access.

[1] European directive 99/93/EC has introduced the term „certification service provider" for TTP's that offer all or some of the services cessary to provide this guarantee.

A Naming and identity, pseudonimity, anonymity

It is usually desirable that the identity of a digital signer is known. This does not mean, however, that this identity must also be stated on the certificate. It is often sufficient that it can be traced if necessary, for instance in the case of fraud. Since the user of a pseudonymous certificate has the apparent intention to keep his identity hidden, it must be very clear exactly which circumstances are sufficient grounds for nonetheless providing these data to others.

Models for 'PET[2] certificates', which protect privacy by using pseudonyms, among other things, deserve more attention than they have received so far. This would help public-key cryptography to realise its potential role as an important privacy-enhancing technology.

Traditional identity data such as name, address, and city of residence are an insufficient basis for reliably linking personal data. Such linking benefits the quality of the data, but may also entail great privacy threats. For this reason the introduction of nationally or even globally unique identifiers to that end is undesirable. Sectoral or chain-based identifiers may provide an alternative solution. Public keys or, even more dangerous, biometric templates, must be prevented from becoming alternative unique identifiers.

B Dissemination of PKI information

Within a PKI it is necessary to disseminate different kinds of information. The most important ones are certificate information and revocation information.

The most popular way of disseminating certificates is through a repository. This should only be done with the permission of the certificate owner, who must also have a real alternative. The permission must be given voluntarily and needs to be based on correct, clear and complete information. When certificates are publicly accessible on a large scale, this opens up all sorts of possibilities for building up detailed profiles. For this reason private dissemination, where the certificate holder himself is responsible for delivering the certificate to a verifying party, deserves serious attention as an alternative.

Revocation information that is disseminated must not contain more data than is necessary, for instance a serial number rather than the entire revoked certificate.

PKI information is disseminated for a certain purpose. Further processing of the information must be compatible with this purpose. This also holds for dissemination by means of a repository; the repository should be designed accordingly.

[2] PET = privacy-enhancing technology.

C Lawful access

Different parties may claim access to data available at TTP's. The desired information may be the identity of the owner of a pseudonymous certificate, keys for decrypting encrypted messages or files, or the messages or files themselves. Law enforcement and intelligence agencies tend to have several specific legal powers in this area. Others usually have lawful access on the basis of a more general right to certain information. The Working Group advocates an approach which balances the investigation needs of governments and their citizens' right to privacy.

The customer's trust is a *conditio sine qua non* for TTP's. It is therefore fashionable in TTP circles to pay lip service to the principles of privacy protection. Unfortunately this rarely goes beyond general remarks along the lines of 'TTP's of course adhere to privacy laws'. Guaranteeing adequate safeguards for personal privacy however requires this aspect to be taken into account from the earliest stages of the designing phase of technologies and infrastructures. If this is done, TTP services in general and digital certificates in particular can provide an important contribution to privacy protection for electronic communication and transactions.

The Working Group therefore makes the following recommendations.

1. Pseudonymous (or even anonymous) certificates are preferable to identity certificates in all cases where identification of the certificate holder is not required in view of the specific purpose for which the certificate is being used. TTP's should contribute actively to the development of technologies and infrastructures allowing for the widest possible use of such certificates, whether within the framework of the X.509 standard or not. In situations where the use of identity certificates cannot be avoided, anonymous or pseudonymous use should be made of such certificates whenever possible.

2. The use of nationally or even globally unique identifiers should be avoided in view of its serious privacy risks. There are alternative possibilities for sectoral or chain-based numbers. Information exchanges based on these should be surrounded with sufficient safeguards. PKI's should be designed in such a way – e.g. by allowing for multiple, short-lived and/or role-based certificates -that certificate numbers, public keys or biometrical templates will not turn into alternative unique identifiers.

3. Public certificate directories should be designed as much as possible in such a way as to allow only those queries that are necessary in view of the purpose of the directory. Individuals should have the choice not to be included in such directories, i.e. private dissemination of certificates must be available to the certificate holder as a real alternative.

4. TTP's may only divulge the identity that goes with a pseudonym in the case of a legal obligation based on a pressing social need or with the express permission of the certificate holder.

5. Powers of investigation services and intelligence services with respect to obtaining lawful access should be in balance with the protection of fundamental rights and freedoms and in particular personal data.

2002

31. Sitzung, 26. und 27. März 2002, Auckland, Neuseeland

Arbeitspapier zur Überwachung der Telekommunikation

In den letzten Monaten haben viele demokratische Staaten neue Befugnisse zur Überwachung der Kommunikation geschaffen, um der Netzkriminalität zu begegnen und den Terrorismus zu bekämpfen. Die Arbeitsgruppe erkennt an, dass angemessene Gegenmaßnahmen ergriffen werden müssen. Sie betont aber auch, dass diese Maßnahmen verhältnismäßig sein müssen. In diesem Zusammenhang erinnert die Arbeitsgruppe daran, dass sie bereits mehrfach bei früheren Gelegenheiten die Bedeutung des Schutzes der Privatsphäre und der persönlichen Kommunikation gegen willkürliche Eingriffe als eines Menschenrechts betont hat (Gemeinsame Erklärung zur Kryptografie vom 12. September 1997 in Paris). Nationales und internationales Recht sollten unmissverständlich klarstellen, dass der Prozess der Kommunikation (z. B. mittels elektronischer Post) ebenfalls durch das Telekommunikationsgeheimnis geschützt ist.

Wenngleich diese Prinzipien die Staaten nicht daran hindern, Netzkriminalität und Terrorismus zu bekämpfen, muss daran erinnert werden, dass z. B. der Europäische Gerichtshof für Menschenrechte wiederholt betont hat, dass Staaten keine unbeschränkte Befugnis haben, Personen in ihrem Zuständigkeitsbereich heimlich zu überwachen. Jedes derartige Gesetz zur heimlichen Überwachung birgt die Gefahr, die Demokratie, die es verteidigen soll, zu untergraben oder gar zu zerstören. „… Staaten dürfen nicht im Namen des Kampfes gegen Spionage und Terrorismus alle Maßnahmen ergreifen, die sie für geeignet halten."[1] Angemessene und wirksame Garantien gegen Missbrauch sind unverzichtbar. Das ist

[1] Europäischer Gerichtshof für Menschenrechte, Fall Klass und andere, Entscheidung vom 18. November 1977, Serie A Nr. 28, S. 23

zusätzlich unterstrichen worden durch den Gemeinsamen Standpunkt der Arbeitsgruppe über die öffentliche Verantwortlichkeit in Bezug auf die Überwachung privater Kommunikation vom 15. April 1998 (Hong Kong)[2].

Vor kurzem hat auch das Europäische Parlament auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hingewiesen, nach der jeder Eingriff in und jede Überwachung der Kommunikation notwendig und verhältnismäßig sein muss; es reicht nicht aus, dass der Eingriff nur nützlich oder wünschenswert ist.

Die Arbeitsgruppe unterstützt die folgenden Vorschläge, die das Europäische Parlament in der Entschließung über die Existenz eines globalen Systems zur Überwachung privater und kommerzieller Kommunikation (ECHELON)[3] gemacht hat und fordert ihre weltweite Umsetzung:

- Staaten sollten ein gemeinsames Schutzniveau gegenüber nachrichtendienstlicher Tätigkeit anstreben und zu diesem Zweck einen Verhaltenskodex ausarbeiten, der sicherstellt, dass die Tätigkeit von Nachrichtendiensten in Übereinstimmung mit den Grundrechten und insbesondere mit dem Schutz der Privatsphäre ausgeübt wird, und sie sollten ein Verfahren der internationalen Kontrolle solcher Aktivitäten vorsehen;

- Staaten sollten ihre Bürger über die Möglichkeit informieren, dass ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; diese Information sollte begleitet werden von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt;

- eine wirksame und effektive Politik betreffend die Sicherheit in der Informationsgesellschaft sollte entwickelt und umgesetzt werden, um auf diese Weise die Sensibilisierung aller Nutzer moderner Kommunikationssysteme für die Notwendigkeit und die Möglichkeiten des Schutzes vertraulicher Informationen zu erhöhen;

- benutzerfreundliche Kryptosoftware, deren Quelltext offen gelegt ist, sollte gefördert, entwickelt und hergestellt werden, da nur so garantiert werden kann, dass keine Hintertüren in Datenverarbeitungsprogramme eingebaut werden;

- öffentliche Verwaltungen sollten elektronische Post systematisch verschlüsseln, sodass langfristig Verschlüsselung zum Normalfall wird,

[2] In diesem Gemeinsamen Standpunkt betonte die Arbeitsgruppe die Notwendigkeit von Verfahren, die der Öffentlichkeit die Gewissheit verschaffen, dass Überwachungsbefugnisse rechtmäßig, angemessen und verhältnismäßig ausgeübt werden.

[3] (A 5 – 0264/2001 (2001/2098) (INI))

- ein Internationaler Kongress zum Schutz der Privatsphäre vor Telekommunikationsüberwachung sollte abgehalten werden, um für Nichtregierungsorganisationen eine Plattform zu schaffen, wo grenzüberschreitende und internationale Aspekte diskutiert und Tätigkeitsfelder und Vorgehen koordiniert werden können.

Die Arbeitsgruppe betont, dass diese Empfehlungen ihre Bedeutung nach den terroristischen Angriffen vom 11. September 2001 nicht eingebüßt haben.

31st meeting, 26th and 27th March 2002, Auckland, New Zealand

Working Paper on Telecommunications Surveillance

In the last months many democratic societies have adopted new powers to intercept communications in order to prevent cyber-crime and obstruct terrorism. The Working Group recognizes that appropriate counter-measures have to be taken. However it also stresses that these measures must be of proportionate nature. In this context the Working Group recalls that it has stressed on several previous occasions the importance of the protection of privacy and personal correspondence against arbitrary intrusions as a human right (Common Statement on Cryptography of 12 September 1997, Paris). National and international law should state unequivocally that the process of communicating (e.g. via electronic mail) is also protected by the secrecy of telecommunications and correspondence.

Although these principles do not prevent governments to take measures to combat cyber-crime and terrorism it should be remembered that e.g. the European Court of Human Rights has constantly stressed that states do not enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. Any such law allowing for secret surveillance poses the danger of undermining or even destroying democracy on the ground of defending it. "…States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[1] Adequate and effective guarantees against abuse are essential. This has been further illustrated by the Working Group's Common Position on Public Accountability in relation to Interception of Private Communications (15 April 1998, Hong Kong[2]).

[1] European Court of Human Rights, Case of Klass and others, Decision of 18 November 1977, Series A no. 28, p.23

[2] In this Common Position the Working Group stressed the need for mechanisms to re-assure the public that interception powers are being used lawfully, appropriately and proportionately.

More recently, the European Parliament too has recalled the jurisprudence of the European Court of Human Rights under which any interference with and interception of communications must be necessary and proportionate; it is not sufficient that the interference is merely useful or desirable.

The Working Group supports the following proposals made by the European Parliament in the resolution on the existence of a global system for the interception of private and commercial communications (ECHELON[3]) and calls for their worldwide implementation:

- States should aspire to a common level of protection with regard to intelligence operations and, to that end, to draw up a Code of Conduct which guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights , in particular with the protection of privacy, and provide for a mechanism of international accountability concerning cross-border surveillance;

- States should inform their citizens about the possibility that their international communications may, under certain circumstances, be intercepted; this information should be accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology;

- An effective and active policy for security in the information society should be developed and implemented, increasing the awareness of all users of modern communications systems of the need to protect confidential information;

- User-friendly open-source encryption software should be promoted, developed and manufactured, as this is the only way of guaranteeing that no backdoors are built into programmes;

- Public agencies should systematically encrypt e-mails, so that ultimately encryption becomes the norm;

- An international conference on the protection of privacy against telecommunications surveillance should be held in order to provide non-governmental organizations with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action.

The Working Group stresses that these proposals have not lost their validity after the terrorist attacks of September 11, 2001.

[3] A5-0264/2001(2001/2098(INI))

Arbeitspapier zum Schutz der Privatsphäre von Kindern im Netz: Die Rolle der elterlichen Einwilligung

Einführung

Die elterliche Einwilligung wird oft dargestellt als Teil der Antwort auf Risiken im Internet, die Kinder und Heranwachsende betreffen, und dies hat seinen deutlichsten Ausdruck im Child Online Privacy Protection Act (COPPA) 1999 in den USA gefunden. Es sind aber Fragen danach aufgeworfen worden, wie die elterliche Einwilligung bezüglich des Datenschutzes richtig eingeordnet werden kann. Der Schutz der Privatsphäre hängt mit der Ausübung der persönlichen Autonomie zusammen, während die elterliche Einwilligung eher ein Modell des „Kindeswohls" widerspiegelt.

Dieses Arbeitspapier versucht nicht, alle Fragen des Online-Datenschutzes von Kindern und jungen Menschen zu behandeln. Es stellt die elterliche Einwilligung und damit zusammenhängende Fragen in den Mittelpunkt. Auch trifft es keine Aussage über die Notwendigkeit oder Angemessenheit der Einholung der elterlichen Einwilligung bei der Bestellung von Waren und Dienstleistungen, was eher grundsätzliche Fragen des Verbraucherschutzes oder Vertragsrechts als des Datenschutzes aufwirft.

Bei der Festlegung, wo die Zustimmung der Eltern erforderlich sein könnte, sollte berücksichtigt werden, dass diese Zustimmung im Zusammenhang mit dem Datenschutz dem Schutz der Interessen des Kindes und nicht der Eltern dient. Die Zustimmung der Eltern sollte nicht zur Voraussetzung gemacht werden, wo das Kind selbst in der Lage ist, eine eigene verständige Entscheidung in der Angelegenheit zu treffen. Es sollte kein Verfahren sein, durch das ein Elternteil die Entscheidung des Kindes korrigieren kann, es sei denn, es besteht die reale Gefahr, dass das Kind die Folgen seiner Entscheidung nicht übersieht oder seine Naivität ausgenutzt wird. Im Wesentlichen sollte die Einwilligung der Eltern verlangt werden, wenn es im Interesse des Kindes liegt, dass eine Entscheidung über die zulässige Verarbeitung seiner Daten getroffen wird, diese Entscheidung aber vernünftigerweise nicht dem Kind allein überlassen werden sollte.

Es ist nicht ganz einfach, allgemeine Grundsätze in praktische Regeln zu übersetzen. Nicht alle Kinder haben die gleichen Fähigkeiten im gleichen Alter (dies kann sogar noch größere Bedeutung erlangen, wenn eine Website auf globaler Basis angeboten wird). Wenn beispielsweise Regeln für ein Kind im Alter von zwölf Jahren und älter festgelegt werden, so kann dies zu restriktiv für manche Kinder sein, aber anderen nicht genug Schutz bieten. Andererseits ist eine Regel, die einen Datenverarbeiter lediglich verpflichtet, bei der Ent-

scheidung über die Erforderlichkeit der elterlichen Einwillligung die Einsichtsfähigkeit des Kindes zu berücksichtigen, in der Praxis nahezu bedeutungslos. Wie könnte ein Datenverarbeiter eine solche Beurteilung treffen, wenn er keine Beziehung zum Kind aufgebaut hat? Eine unbestimmte Regel führt zu unterschiedlichen Maßstäben in vergleichbaren Umständen und kann von skrupellosen Geschäftsleuten ausgenutzt werden. Sogar eine strikte Altersgrenze führt zu Problemen. Wie könnte ein Datenverarbeiter online das Alter einer Person feststellen, die seine Website aufruft? Könnte die Einführung von Verfahren zur Verifikation solcher Einzelheiten Datenschutzrisiken in anderen Zusammenhängen auslösen?

Kinder sind durchaus in der Versuchung, falsche Angaben zu machen, wenn damit ein Vorteil verbunden zu sein scheint. Das bedeutet nicht, dass es von vornherein wertlos ist, ein Kind nach seinem Alter zu befragen, aber die Möglichkeit, dass das Kind nicht wahrheitsgemäß antwortet, sollte in Betracht gezogen und vom Datenverarbeiter nicht ausgenutzt werden. Eine vorsichtige Herangehensweise könnte darin bestehen, sicherzustellen, dass die Folgen einer Entscheidung nicht dazu führen, dass ein Kind auf Grund falscher Altersangaben einer völlig unangemessenen Verwendung seiner Daten ausgesetzt wird.

Es ist eingewandt worden, dass eine elterliche Einwilligung, die nicht verifiziert werden kann, wertlos ist. Darüber gibt es allerdings unterschiedliche Auffassungen. Selbst wenn ein Kind ohne weiteres behaupten kann, die Eltern hätten zugestimmt, obwohl sie dies in Wahrheit nicht getan haben, bewirkt schon das Stellen der Frage nach der elterlichen Einwilligung einen gewissen (begrenzten) Schutz (man denke nur an die Situation in einer Offline-Umgebung, wo die meisten Kinder sich hüten werden, einem Lehrer gegenüber wahrheitswidrig anzugeben, ihre Eltern hätten eingewilligt, wenn das später möglicherweise herauskommt). Es mag Situationen geben, in denen die zulässige Erhebung von Daten dadurch hinreichend sichergestellt werden kann, dass das Kind vor die Frage gestellt und in eine Lage gebracht wird, in der es lügen müsste, wenn es ohne Einwilligung der Eltern weiter surfen und mit der Offenbarung von Daten auf einer Website fortfahren würde. In den meisten Fällen, in denen die elterliche Zustimmung das angemessene Kriterium ist, muss sie jedoch auch verifizierbar sein. Das ist in der Praxis offensichtlich schwierig sicherzustellen. Die Tatsache, dass es unpraktikabel oder unverhältnismäßig schwierig ist, eine verifizierbare elterliche Einwilligung zu erhalten, sollte das Kind nicht einem Risiko aussetzen. Wenn der Datenverarbeiter nicht in der Lage oder nicht bereit ist, sich um eine Verifizierung der Einwilligung zu bemühen, sollte dies nicht als Grund dafür angesehen werden, um einen weniger strengen Maßstab anzulegen. Die Konsequenz der mangelnden Bereitschaft des Datenverarbeiters muss sein, dass er von einer verweigerten Einwilligung auszugehen hat.

Wann kann die Einwilligung der Eltern verlangt werden?

Unter welchen Umständen ist es angemessen, die Einwilligung der Eltern einzuholen?

- Wenn ein Kind aufgefordert wird, personenbezogene Daten anzugeben – je nach dem Alter des Kindes und der Art des Geschäftszweckes des Datenverarbeiters kann sich dies auf die Angabe jeder Information oder nur von bestimmten Informationen beziehen (wie z. B. sensible Daten, die nur zur Unterstützung von Marketingaktivitäten benötigt werden);

- wenn ein Datenverarbeiter die Weitergabe der Information über das Kind oder ihre Zweckentfremdung insbesondere für Werbezwecke plant;

- wenn die personenbezogene Information über ein Kind auf einer Website veröffentlicht werden soll.

Grundsätzlich erscheint es nicht angemessen, das Einverständnis der Eltern einzuholen, wenn das Kind sein Auskunftsrecht online ausüben will.

Schlussfolgerungen

Die Arbeitsgruppe ist sich dessen bewusst, dass es nicht möglich ist, einen abschließenden Katalog von Maßstäben zu entwickeln, die für die elterliche Einwilligung zur Online-Erhebung von Daten über Kinder eindeutig, praktikabel und weltweit angewandt werden können. Darüber hinaus vertritt die Arbeitsgruppe die Auffassung, dass ethische Geschäftsgrundsätze und die strikte Befolgung von allgemeinen anerkannten Datenschutzprinzipien die Notwendigkeit verringern werden, auf die elterliche Einwilligung zurückzugreifen.

Dennoch ist die Arbeitsgruppe der Ansicht, dass diejenigen, die personenbezogene Daten im Zusammenhang mit Online-Aktivitäten von Kindern verarbeiten, sich an folgenden Grundsätzen orientieren sollten.

Im Zusammenhang mit dem Datenschutz sollte das elterliche Einverständnis nur dann als Instrument zum Schutz der Privatsphäre des Kindes genutzt werden, wenn dieses Ziel nicht sinnvoll erreicht werden kann, ohne einen Interessenvertreter des Kindes an der Entscheidung zu beteiligen. Dies sind typischerweise die Eltern. Das Einverständnis der Eltern sollte kein Mittel der elterlichen Kontrolle über ein Kind in solchen Situationen sein, in denen der Schutz der Privatsphäre des Kindes die Beteiligung der Eltern nicht erfordert.

Die Arbeitsgruppe gibt den Datenverarbeitern die folgenden Empfehlungen als Richtschnur, die in vielen Fällen die Anforderungen des Datenschutzes erfüllen wird. Die Empfehlungen müssen möglicherweise dem nationalen Recht und den besonderen Umständen angepasst werden, unter denen verantwortliche Stellen Daten von Kindern verarbeiten:

– Wenn personenbezogene Daten genutzt werden, um Mitteilungen an Kinder zu versenden, die jünger als sechzehn Jahre sind oder die wahrscheinlich von besonderem Interesse für Kinder sind, sollte die Mitteilung altersangemessen sein und nicht die Leichtgläubigkeit, mangelnde Erfahrung und den Loyalitätssinn von Kindern ausnutzen.

– Personenbezogene Daten sollten bei Kindern nur mit der ausdrücklichen und verifizierbaren Einwilligung der Eltern (einschließlich der Betreuer oder Sorgeberechtigten) erhoben werden, es sei denn:

  a) das Kind ist zwölf Jahre alt oder älter und

  b) die erhobenen Daten beschränken sich auf das, was notwendig ist, um dem Kind weitere rechtmäßige Mitteilungen online zu übermitteln und

  c) das Kind versteht, was das bedeutet.

– Personenbezogene Daten, die bei einem Kind erhoben worden sind, sollten nicht ohne ausdrückliche und überprüfbare Zustimmung der Eltern des Kindes an Dritte weitergegeben werden.

– Personenbezogene Daten über Dritte (z. B. Eltern) sollten nicht bei Kindern erhoben werden.

– Die Veröffentlichung oder Weitergabe von personenbezogenen Daten über Kinder sollte nicht ohne die ausdrückliche und überprüfbare Einwilligung der Eltern des Kindes erfolgen.

– Kinder sollten nicht durch die Aussicht auf einen Gewinn oder ähnliche Anreize zur Preisgabe personenbezogener Daten verleitet werden.

– Die Verarbeitung der Daten von Kindern sollte nur für eine begrenzte Zeit auf die elterliche Einwilligung gestützt werden. Wenn eine Person volljährig wird oder eindeutig die Fähigkeit erlangt, die erforderlichen Entscheidungen selbst zu treffen, sollte die Verarbeitung der Daten auf die Entscheidungen der betroffenen Person selbst statt auf die ihrer Eltern gestützt werden.

Das Erfordernis, das elterliche Einverständnis einzuholen, verdrängt nicht andere Erfordernisse des anwendbaren Datenschutzrechts, z. B.

– eine Verpflichtung, auch die Zustimmung des Kindes einzuholen,

– Begrenzungen der Weiterverwendung von Informationen, die das Kind offenbart hat.

Working Paper on Childrens' Privacy On Line: The Role of Parental Consent

Introduction

Parental authorisation is often presented as part of a response to on-line issues affecting children and young people and this had been seen most explicitly in the Children's On-line Privacy Protection Act 1999 in the United States. However, questions have been raised as to how parental consent properly is to be seen in terms of privacy and data protection. Privacy involves the exercise of personal autonomy whereas parental consent might better be seen as reflecting a "best interest" or "child protection" model.

This paper does not attempt to canvass all on-line privacy issues for children and young people. It focuses on parental consent and related matters. Nor is it concerned with the merits or otherwise of requiring parental consent before ordering goods or services, which principally raises issues of consumer protection or contract rather than data protection.

In determining where parental consent might be required, it should be borne in mind that the purposes of consent, in a data protection context, is to protect the interests of the child not of the parent. Parental consent should not be a requirement where a child is capable of taking its own rational decision on the relevant matter. It should not be a mechanism through which a parent can override the child's decision unless there is a real risk the child does not appreciate the consequences of the decision or the child's naivety is being exploited. Essentially, parental consent should be required where it is in the interests of the child that a decision on fairly processing his/her personal data is taken but the decision cannot reasonably be left to the child alone.

There is some difficulty with translating general principles into practical rules. Not all children have the same ability at the same age. (This may be even more marked when a web site operates on a global basis.) For example, a standard set for a child 12 years and above may be overly restrictive for some children but insufficiently protective for others. On the other hand, a rule that simply states that a data controller must take the ability of a child into account in deciding whether parental consent is required is almost meaningless in practice. How could a data controller make such judgments unless it has an established relationship with the

child? A vague rule will lead to different standards being applied in equivalent circumstances and is open to exploitation by unscrupulous traders. Even an age-based rule has problems. How, in the on-line world could a data controller know the age of a person accessing its website? Might the establishment of mechanisms to verify such details create privacy risks in other contexts?

Children might well be tempted to give wrong information if there is some perceived benefit that accrues from doing so. This does not mean that asking a child his/her age is of no value but the possibility that children will not tell the truth should be recognised and not exploited by data controllers. A cautious approach might be to ensure that the consequences of the decision not be such that there is a risk that a child who gives a false age will be exposed to totally inappropriate use of his/her personal data.

It has been suggested that unless parental consent is "verifiable" it is of no value. However, views differ on this point. Although a child can easily say that parents have consented when they have not, simply asking the question provides some (limited) protection. (Consider the off-line environment where most children will be wary of telling a teacher that their parents have consented if they might get caught out later.) There may be cases where asking a question and putting children in the position where they have to lie if they are to proceed without parental consent will be sufficient measure to ensure fair processing of personal data. However, in most cases where parental consent is the appropriate standard it is necessary for the consent to be verifiable. This is clearly difficult to achieve in practice. The fact that obtaining verifiable parental consent may be impracticable or require disproportionate effort should not place the child at risk. If a data controller is unable or unwilling to make the effort to verify consent, then this should not be seen as a reason for adopting a less restrictive standard. The consequences of the data controller's unwillingness must be that they can then only proceed as if consent has been denied.

When might parental consent be required?

In what circumstances might it be appropriate to obtain parental consent?

- where a child is asked to provide personal data – depending on the age of the child and the nature of the data controller's business this might be the provision of *any* information or only of *certain* information (such as sensitive data or that which is solely required to support marketing activities);

- where a data controller intends to disclose information about the child or use it for a different purpose, typically direct marketing;

- where identifiable information about a child is to be published on a website.

Generally it would not seem appropriate to require parental consent:

- to exercise a subject access right on-line.

Conclusions

The IWGDPT recognises that it is not possible to develop a single set of standards for the application of parental consent to the processing of children's personal data on-line that are clear, practical and applicable worldwide. Furthermore it considers that ethical business practices and the rigorous adherence to generally accepted data protection principles will diminish the need to resort to parental consent.

Nevertheless the IWGDPT takes the view that those processing personal data in connection with children's on-line activities should be guided by the following principle.

In a data protection context, parental consent should only be used as a mechanism for protecting a child's privacy where this aim cannot reasonably be achieved without involving someone to represent the child's best interests in decision-making. Typically this is a parent. Parental consent should not be a mechanism to enable parents to exercise control over a child in circumstances where the protection of the child's privacy does not require the parent's involvement.

The IWGDPT makes the following suggestions to data controllers as a benchmark which will in many cases satisfy data protection requirements. The suggestions may need to be adapted in the light of the particular circumstances in which data controllers process children's personal data and the applicable national law:

– Where personal data are used to send communications directed at children (individuals under 16 years of age) or likely to be of particular interest to children, the communications should be age appropriate and should not exploit the child's credulity, lack of experience or sense of loyalty.

– Personal information should only be collected from children with the explicit and verifiable consent of the child's parent (including guardian or principal caregiver) unless:

  a. the child is aged 12 years or over and

  b. the information collected is restricted to that necessary to enable the child to be sent further lawful on-line communications and

  c. the child understands what is involved.

– Personal information collected from children should not be disclosed to third parties without the explicit and verifiable consent of the child‘s parent.

– Personal information relating to other people (for example parents) should not be collected from children.

– The public display or distribution of personal information about children should not occur without the explicit and verifiable consent of the child‘s parent.

– Children should not be enticed to divulge personal information with the prospect of a game prize or similar inducement.

– Reliance on parental consent for processing a child‘s data should be time limited. When an individual ceases to be a child or becomes clearly capable of making the relevant decisions him/herself, processing should be based on the individual‘s own decisions not those of his/her parents.

A requirement to obtain a parent’s consent does not override other requirements of applicable data protection law, for example

– A requirement to also obtain the child’s consent

– Limitations on secondary use of the information provided by the child.

Arbeitspapier zur Nutzung eindeutiger Identifikatoren in Telekommunikationsendgeräten: Das Beispiel IPv6

Aufgrund einer vorhersehbaren Verknappung in dem gegenwärtig für die meisten Internetverbindungen genutzten Protokoll (IP Version 4) ist durch die Internationale Internet Engineering Task Force (IETF) eine Veränderung des Protokolldesigns ausgearbeitet worden. Dieses neue Protokoll IPv6 nutzt eine Ziffernfolge von 128 Bit anstatt der 32 Bit in der vorherigen Version zur Darstellung individueller IP-Adressen im Internet.

Diese neue Adressierung beinhaltet aufgrund ihrer vergrößerten Kapazität viele Vorteile und ermöglicht neue Dienste wie Multicasting (schnelle Übertragung von großen Datenmengen zu einer Vielzahl von Empfängern, z. B. Video on-line), voice over IP usw.

Allerdings erweckt das neue Protokoll auch Bedenken, da es so beschaffen ist, dass jede IP-Adresse teilweise aus einer eindeutigen Nummernfolge wie einem globalen, eindeutigen Identifikator zusammengesetzt werden kann. Die Einführung von IPv6 könnte zu erhöhten Risiken der Profilbildung von Nutzeraktivitäten im Internet führen[1].

Die folgenden vorläufigen Überlegungen identifizieren die Risiken und verweisen auf die Datenschutzgrundsätze, die in Betracht gezogen werden müssen, wenn eindeutige Identifikatoren bei der Bildung von IP-Adressen genutzt werden.

I. Identifizierte Risiken

Die Charakteristiken von IPv6 bedingen spezifische Risiken für die Privatsphäre, die von der Art der Konfiguration des neuen Protokolls abhängig sind.

- Probleme der Profilbildung stehen zur Debatte, wenn ein eindeutiger Identifikator (die Kennung der Schnittstelle, die z. B. auf der eindeutigen MAC-Adresse einer Internet-Karte basieren kann) in die IP-Adresse jeder elektronischen Kommunikationseinrichtung eines Nutzers integriert wird. In diesem Fall kann die gesamte Kommunikation viel einfacher, als dies unter Nutzung von Cookies heute der Fall ist, zusammengeführt werden.

- Es können Probleme der Sicherheit und der Vertraulichkeit festgestellt werden. Diese Risiken hängen mit der Entwicklung neuer Netzwerkdienste zusammen, die die Vervielfachung der Endgeräte beinhalten, die mit dem Netzwerk über dasselbe Kommunikationsprotokoll verbunden sind: Mobiltelefone, Personalcomputer, elektronische Agenten zur Kontrolle von Haushaltsgeräten (Heizung, Licht, Alarmanlagen usw.).

Das neue IPv6-Protokoll ermöglicht dauerhafte Verbindungen, bei denen sogar in den Fällen, in denen ein Endgerät innerhalb des Netzwerkes versetzt wird, dieselbe Adresse beibehalten wird. Hier spielen Aspekte der Sicherheit und der Vertraulichkeit eine Rolle, da ein Risiko der Identifikation von Aufenthaltsinformationen dieser mobilen Knoten existiert[2].

[1] Die zusammenhängende Profilbildung über Aktivitäten eines Nutzers könnte sogar möglich sein, wenn dieselben Endeinrichtungen in verschiedenen Netzen genutzt werden.

[2] vgl. A. Escudero Pascual „Anonymous and untraceable communications: location privacy in mobile internetworking", 16. Mai 2001; "Location privacy in IPv6 – Tracking the binding updates", 31. August 2001; http//www.it.kth.se/~aep/.

II. Auf IPv6 anwendbare Datenschutzprinzipien

Die Arbeitsgruppe hält es für erforderlich, die Aufmerksamkeit aller Beteiligten, die für die Ausarbeitung und Implementierung des neuen Protokolls verantwortlich sind, auf die nationalen und internationalen gesetzlichen Anforderungen zum Datenschutz und zur Sicherheit der Telekommunikation zu lenken.

Es ist heute weithin anerkannt, dass eine IP-Adresse – und *a fortiori* eine eindeutige Identifikationsnummer, die in die Adresse integriert ist – als personenbezogenes Datum im Sinne der gesetzlichen Bestimmungen angesehen werden kann[3].

Im Einklang mit ihrer bisherigen Arbeit und den gemeinsamen Standpunkten, die zu dieser Problematik bereits verabschiedet worden sind[4], erinnert die Arbeitsgruppe an die folgenden Prinzipien, die bei der Implementierung des neuen Internet-Protokolls in Betracht gezogen werden sollten.

Telekommunikationsinfrastruktur und technische Geräte müssen so konstruiert sein, dass entweder überhaupt keine personenbezogenen Daten oder so wenig personenbezogene Daten wie technisch möglich genutzt werden, um Netze und Dienste zu betreiben. Ein eindeutiger Identifikator einer Schnittstelle, wie er in IPv6 integriert ist, würde einen Identifikator zur generellen Anwendung darstellen.

- Im Gegensatz zum Prinzip der Datenminimierung würde eine derartige Nutzung eines eindeutigen Identifikators ein Risiko zur Bildung von Profilen Einzelner über all ihre Aktivitäten im Zusammenhang mit einem Netzwerk bilden.

- Der Schutz des Grundrechts auf Datenschutz gegen solche Risiken der Profilbildung muss bei der Analyse der verschiedenen Aspekte des neuen Protokolls, wie seiner Handhabbarkeit**,** als oberster Grundsatz gelten.

- Verbindungsdaten, und insbesondere Aufenthaltsinformationen, verdienen aufgrund ihres sensiblen Charakters einen besonderen Schutz[5].

---

[3] vgl. z. B. auf der europäischen Ebene die Mitteilung der Kommission «Organisation und Verwaltung des Internet – Internationale und europäische Grundsatzfragen 1998 – 2000» KOM (2000) 202 endg. vom April 2000, und die von der Datenschutz-Arbeitsgruppe nach Art. 29 verabschiedeten Dokumente, besonders „Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz“, WP 37, 21. November 2000.

[4] Gemeinsamer Standpunkt zu Online-Profilen im Internet, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000; Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16. Februar 2001; Zehn Gebote zum Schutz der Privatheit im Internet – Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz, angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14. September 2000.

[5] vgl. Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, angenommen auf der 29. Sitzung der Arbeitsgruppe am 15./16. Februar 2001.

Wenn Aufenthaltsinformationen bei der Nutzung mobiler Endgeräte und anderer Objekte, die über IP verbunden sind, erzeugt werden müssen, müssen diese Informationen gegen unrechtmäßiges Abhören und Missbrauch geschützt werden. Es sollte auch verhindert werden, dass Aufenthaltsinformationen (und die Veränderung dieser Aufenthaltsinformationen aufgrund der Bewegung des mobilen Benutzers) unverschlüsselt zum Empfänger dieser Informationen über den „Header" der genutzten IP-Adresse übertragen werden.

Protokolle, Produkte und Dienste sollten so beschaffen sein, dass sie Wahlmöglichkeiten für permanente oder veränderbare Adressen bieten. Die Grundeinstellungen sollten für ein hohes Maß an Datenschutz sorgen.

Da diese Protokolle, Produkte und Dienste sich ständig weiterentwickeln, wird die Arbeitsgruppe diese Entwicklungen genau beobachten und, soweit dies notwendig ist, zu einer spezifischen Regulierung aufrufen.

Working paper on the use of unique identifiers in telecommunication terminal equipments: the example of Ipv6

Due to a forseeable shortage in the protocol used today for most of the Internet connections (Ip version 4), a change of design in the protocol has been elaborated by the international Internet Engineering Task Force (IETF). This new protocol, IPv6, uses a string of 128 bits instead of 32 bits in the former version, to constitute each individual IP address on the Internet[1].

This new address, thanks to its enlarged capacities, presents many advantages and enables new facilities such as multicasting (quicker transmission of large amounts of data to multiple recipients, e.g. video on-line), voice over IP, etc.

However, the new protocol also raises concerns, as it has been designed in such a way that each IP address can be partly constituted of a unique serie of numbers like a global unique identifier. The introduction of IPv6 might lead to increased risks of profiling of user activities on the Internet.

The following preliminary considerations identify the risks and recall the privacy principles to take into consideration while using a unique identifier in the constitution of IP addresses.

[1] Overall profiling of activities of a user might even be feasible when the same terminal equipment is used in different networks.

I. Identified risks

The characteristics of IPv6 lead to the identification of specific privacy risks, which will depend on the configuration of the new protocol.

- *Profiling issues* are at stake if a unique identifier (the interface identifier e.g. based on the unique MAC address of the ethernet card) is integrated in the IP address of each electronic communication device of the user. In such case, all communications of the user can be linked together, much easier than using cookies as they exist today.

- *security and confidentiality issues* can be identified. These risks are linked with the development of network services, which implies multiplication of the type of terminals connected to the network using the same communication protocol: mobile phones, personal computers, electronic agents controlling home devices (heating, light, alarms, etc.).

The new Ipv6 protocol allows stable connections, with maintenance of the same address, even when a terminal is moving on the network. Security and confidentiality aspects are at stake here, as there is a risk of identification of location data of this mobile node[2].

II. Data protection principles applicable to Ipv6

The working group deems it necessary to draw the attention of all the actors responsible in the elaboration and the implementation of the new protocol, about the national and international legal requirements governing privacy and security of telecommunications.

It is now widely recognised that IP address – and *a fortiori* a unique identification number integrated in the address – can be considered as personal data in the sense of the legal framework[3].

[2] See e.g. A. Escudero Pascual, "Anonymous and untraceable communications: location privacy in mobile internetworking", 16 May 2001; "Location privacy in Ipv6 – Tracking the binding updates", 31 August 2001; http://www.it.kth.se/~aep/

[3] See e.g. at European level, the Communication of the Commission on the Organisation and Management of the Internet Domain Name System of April 2000, and the documents adopted by the art. 29 data protection working party, in particular "Privacy on the Internet – An integrated EU Approach to On-line Data Protection", WP 37, 21 Nov. 2000.

In line with its previous work and the common positions already adopted on that subject[4], the Working Group recalls the following principles, which should be taken into account while implementing the new Internet protocol.

Telecommunications infrastructure and technical devices have to be designed in a way that either no personal data at all or as few personal data as technically possible are used to run networks and services. The unique identifier of an interface as integrated in IPv6 would constitute an identifier of general application.

- In contradiction with the principle of data minimisation, such use of a unique identifier constitutes a risk of profiling of individuals for all their activities in connection with a network.

- The protection of the fundamental right to privacy against such risk of profiling must prevail while analysing the different aspects of the new protocol, such as its facility of management.

- Traffic data, and in particular location data, deserve a specific protection considering their sensitive character[5].

If location information has to be generated in the framework of the use of mobile devices and other objects connected via IP, such information must be protected against unlawful interception and misuse. It should also be avoided that the location information (and the changing in this location information depending on the movement of the mobile user), is transmitted non encrypted to the recipient of the information via the header of the IP address used.

Protocols, products and services should be designed to offer choices for permanent or volatile addresses. The default settings should be on a high level of privacy protection.

Since these protocols, products and services are continuously evolving the Working Group will have to monitor closely the developments and to call for specific regulation if necessary.

[4] Common Position regarding Online Profiles on the Internet adopted at the 27th meeting of the Working Group on 4/5 May 2000; Common Position on Privacy and location information in mobile communications services adopted at the 29th meeting of the Working Group on 15/16 February 2001; Ten Commandments to protect Privacy in the Internet World Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements adopted at the 28th meeting of the Working Group on 13/14 September 2000.

[5] See the Common Position on Privacy and location information in mobile communications services adopted at the 29th meeting of the Working Group on 15/16 February 2001.

Arbeitspapier zur netzwerkbasierten Telemedizin

– aktualisiert auf der 38. Sitzung am 6./7. September 2005 in Berlin –

Telemedizin ist das Praktizieren von Medizin aus der Entfernung. Der Begriff ist weit genug gefasst, um den australischen „Flying Doctor Service", Fernuntersuchungen über Video nach Unfällen auf Bohrinseln und medizinische Ratgeber-Sendungen im Fernsehen oder im Radio zu umfassen. Dieses Papier beschäftigt sich mit netzwerkbasierten Gesundheitsdiensten und ihren Implikationen für den Datenschutz.

Die „American Medical Association" hat festgestellt, dass „der Zugang zu medizinischer Information über das Internet das Potenzial besitzt, die Beziehung zwischen Arzt und Patient von der ärztlichen Autorität, die Behandlungen und Beratung verabreicht zu einem gemeinsamen Entscheidungsprozess zwischen Patient und Arzt zu beschleunigen[1]. Andere mögen nicht so optimistisch sein. Die Zunahme von Informationsangeboten zur Gesundheit im Internet[2], Online-Selbsthilfe- und Diskussionsgruppen[3] und die elektronische Übermittlung von Gesundheitsdaten über das Internet erweckt den Eindruck, dass das Internet ein integraler Bestandteil der Gesundheitsversorgung werden wird.

Das Angebot von Gesundheitsdiensten über das Internet findet gegenwärtig in drei Umgebungen statt:

1. Das Internet als ein Forum für die Diskussion von Gesundheitsfragen

Dies schließt Internet-basierte Diskussionsgruppen und Mitteilungsdienste ein. Die Veröffentlichung kann anonym sein und die Diskussionen werden entweder moderiert oder nicht. Informationen, die in diesen Foren veröffentlicht werden, tendieren dazu, eher anekdotischer als verlässlicher Natur zu sein und schließen normalerweise nicht die Bezahlung einer Gebühr oder eines Abonnements oder die Begründung einer klinischen Beziehung zwischen dem Informationsanbieter und dem Informationssucheden ein. Auf der professionellen Ebene existieren private Diskussionsgruppen, für die eine Gebühr erhoben wird und bei denen die Aufnahme auf eine bestimmte Untergruppe der Internetnutzer wie z. B. Ärzte beschränkt ist.

[1] American Medical Association, "Guidelines for Medical and Health Information Sites on the Internet", http://www.ama-assn.org/ama/pub/category/1905.html

[2] vgl. www.medscape.com, ein Portal, das an Ärzte und interessierte Laien gerichtet ist.

[3] vgl. die Untersuchung über medizinische Internetnutzung www.hon.ch/Survey/FebMar2001/survey.html

2. Internet-basierte Erbringung von Gesundheitsdiensten von Ärzten für Patienten (e-Ärzte)

Es hat einige Versuche gegeben, die traditionelle Arzt-Patient-Beziehung in der virtuellen Welt abzubilden. Patienten, die sich unter Umständen zu einem bestimmten Zeitpunkt für Abrechnungszwecke identifizieren müssen, übermitteln private Anfragen mit der Beschreibung ihrer Symptome an Ärzte. Der Arzt, dessen Name und Qualifikation in dem Internetangebot verfügbar ist, kann durch e-Mail oder gesicherte Internetverbindungen antworten, berät und schlägt eine Behandlung vor. Obwohl es dem Arzt nicht möglich sein wird, seinen Patienten zu berühren, könnte eine visuelle Untersuchung durch die Nutzung einer Webcam möglich sein (obwohl dies bisher nicht üblich ist). Nationale Gesetze werden typischerweise fordern, dass Rezeptverordnungen die Unterschrift des Arztes tragen, und es mag in manchen Fällen unethisch sein, Medikamente zu verschreiben, ohne den Patienten persönlich untersucht zu haben[4].

3. Das Internet als Aufbewahrungsort für Patientenakten

In manchen Fällen existiert als Teil des unter 1. und 2. Beschriebenen ein elektronisches Archiv personenbezogener Gesundheitsdaten, zu denen der Betroffene und sein autorisierter Behandler Zugang haben.

Dieses Papier beschäftigt sich mit der Internet-basierten Erbringung von Gesundheitsdiensten.

Eine Auswahl von Datenschutzproblemen bei Internet-basierter Telemedizin

Ethische Verpflichtungen und gesetzliche Pflichten zur Vertraulichkeit

Ein eingeführter Bestandteil der normalen Beziehung zwischen Arzt und Patient ist die Vertraulichkeit. Vertraulichkeit zwischen Arzt und Patient verpflichtet den Arzt im Hinblick auf die persönlichen Informationen des Patienten. Wenn ein zugelassener Arzt Gesundheitsdienstleistungen erbringt, gelten gleichzeitig ethische Beschränkungen, unabhängig davon, ob die Arztpraxis tatsächlicher oder virtueller Natur ist. Allerdings müssen einige spezifische Probleme in Bezug auf den Datenschutz der Nutzer von on-line-Gesundheitsdiensten bei der Nutzung des Internet betrachtet werden.

Probleme können sich aus der Nutzung von Verbindungsdaten ergeben, die im Zuge einer Interaktion zwischen Arzt und Patient entstehen. Verbindungsdaten

[4] Apotheker dürfen Medikamente verkaufen, solange sie eine Verordnung erhalten (sie brauchen den Betroffenen dafür nicht sehen zu können). Als Beispiel eines Internet-basierten Verkäufers vgl. „CyberChemist“ unter www.chemist.co.nz/pm/index.cfm.

können unter bestimmten Umständen mit Daten über andere Nutzungen des Internet und personenbezogenen Daten zusammengeführt werden. Daten über Verordnungen sind z. B. für Hersteller von Medikamenten von Interesse. Ein weiteres Anliegen ist Grundvertrauen. Nutzer müssen überzeugt sein, dass eine Webseite ein vertrauenswürdiger Aufbewahrungsort für ihrer medizinischen Daten ist.

Wenn Internet-Angebote dieser Art Erfolg haben sollen, muss das Internet zunächst als ein akzeptabler Weg für die Erbringung von Gesundheitsdiensten angesehen werden. Datenschutz ist eines der wichtigsten Bedenken der Nutzer im elektronischen Geschäftsverkehr und die Sensibilität von Gesundheitsinformationen vergrößert diese Bedenken. Es sind einige Versuche unternommen worden, gute Praktiken und dadurch das Vertrauen der Öffentlichkeit zu fördern. Ein Beispiel ist der "Health On-Line Code of Conduct", der verlangt, dass Internetangebote „die gesetzlichen Anforderungen hinsichtlich des Datenschutzes bei medizinischer oder Gesundheits-Information beachten, die in demjenigen Land oder Bundesstaat gelten, in dem das Internet-Angebot und gespiegelte Angebote angesiedelt sind oder darüber hinausgehen"[5]. Ein anderes Beispiel bilden die AMA „Guidelines for Medical and Health Information Sites on the Internet"[6]. Solche Initiativen werden in manchen Fällen durch selbstregulierende Datenschutz-Gütesiegel-Programme mit externer Zulassung und Beschwerde-Verfahren unterstützt.

Erhebung, Nutzung und Übermittlung

Die Erhebung von Daten während einer telemedizinischen Untersuchung kann – anders als bei einer „physikalischen" Untersuchung – indirekt oder sogar „unsichtbar" erfolgen. Internetangebote veröffentlichen oft Datenschutzerklärungen, die Aussagen darüber enthalten, welche Daten erhoben werden[7], aber diese decken nur selten die Nutzung von „Third Party Cookies" ab, die durch Werbeunternehmen platziert werden. Die Weiterverwendung von Verbindungsdaten, besonders wenn diese mit anderen personenbezogenen Daten kombiniert werden, würde ein ernsthaftes Problem darstellen. Es ist unwahrscheinlich, dass Probleme im Zusammenhang mit Verbindungsdaten oder Cookies durch herkömmliche ethische Regelung angemessen geregelt werden. Dies könnte verstärkt werden durch eine enge Partnerschaft, die zwischen praktischen Ärzten und Medikamentenherstellern existieren könnte.

[5] vgl. www.hon.ch. Ein Artikel aus dem „Journal of Medical Internet Research", der diesen Code kritisiert, ist verfügbar unter www.jmir.org/2000/1/37

[6] s. Fußnote 1

[7] Eine Studie, nach der eine Inkonsistenz zwischen den veröffentlichten Datenschutzerklärungen von Angeboten zur Gesundheit im Internet und deren tatsächlicher Praxis besteht, kann abgerufen werden unter www.ehealth.chcf.org/view.cfm?itemID=12497

Ethische Probleme und Datenschutzprobleme können auch entstehen, wenn Verbindungsdaten zu Forschungszwecken mit personenbezogenen Daten der Patienten zusammengeführt werden.

Angemessenheit

Es kann Aspekte medizinischer Beratung geben, für die Internet-basierte Anwendungen für die vorhersehbare Zukunft unangemessen sind. Dies gilt z. B. in Fällen, in denen eine Diagnose ohne weitere Informationen durch den Patienten nicht sicher vorgenommen werden kann (obwohl die Einholung einer „zweiten Meinung" möglich sein wird, solange der untersuchende Arzt die Symptome und den Zustand bereits sorgfältig aufgezeichnet hat).

Sicherheit

Sicherheitsprobleme existieren bei der Speicherung medizinischer Daten, so dass Ärzte und Patienten über das Internet darauf zugreifen können. TCP/IP ist ein in sich unsicheres Medium[8] und Methoden zur Beseitigung dieser Unsicherheit verlangen Maßnahmen und finanziellen Aufwand in dem Internetangebot, in dem die Daten gespeichert werden. Während die Online-Speicherung von medizinischen Informationen eine gute Nutzung der Allgegenwärtigkeit des Web darstellt, entsteht durch sie auch die Möglichkeit eines Fernzugriffs von unsicheren Orten wie Internet-Cafes.

Die Vertraulichkeit medizinischer Informationen wird von den Nutzern als sehr wichtig eingeschätzt und wirksame Sicherheitsmaßnahmen gegen unautorisierten Zugriff stellen eine unverzichtbare Maßnahme dar, um den Bruch der Vertraulichkeit zu verhindern. Sie können gleichzeitig auch einen Wettbewerbsvorteil für jegliches Internetangebot zur Telemedizin bilden.

Vorteile

Wie nicht anders zu erwarten, hat sich dieses Papier auf die Problembereiche konzentriert. Bevor Empfehlungen gegeben werden, soll auf Aspekte Internet-basierter Telemedizin hingewiesen werden, die zu einer Verbesserung des Datenschutzes führen können:

- Der Einzelne kann in die Lage versetzt werden, selbst auf Informationen zugreifen zu können; sowohl auf die eigenen Patientenakten als auch auf Gesundheitsratgeber, und zwar zu praktisch jeder Zeit und an jedem Ort in der Welt;

[8] Für eine kurze Erläuterung der Hintergründe s. www.itsecurity.com/tutor/tcpip.htm

- Internet-basierte Telemedizin eröffnet anonyme Möglichkeit, eine „zweite Meinung“ einzuholen – manche Betroffenen hatten Hemmungen oder es war ihnen peinlich, eine zweite Meinung in der traditionellen Weise durch ihren eigenen Arzt zu verlangen;

- Cyber-Apotheken bilden das moderne Äquivalent der Katalogbestellung und können die Verlegenheit beim Ausfüllen von Verordnung für Medikamente gegen sexuell übertragbare Krankheiten etc. – besonders in Kleinstädten – verringern.

Empfehlungen

Aus der Sensitivität medizinischer Daten folgt, dass die gesetzlichen Bestimmungen zum Datenschutz von Anbietern Internet-basierter Telemedizin genauestens eingehalten werden müssen. Wo solche gesetzlichen Regelungen nicht anwendbar sind, sollten die allgemein anerkannten Prinzipien des fairen Umgangs mit Informationen beachtet werden und jegliche Erhebung, Nutzung und Übermittlung von Daten sollte mit der informierten Einwilligung des Betroffenen erfolgen. Zusätzlich zu den üblichen Datenschutzerwägungen werden folgende Empfehlungen gegeben:

1. Internetangebote zur Telemedizin müssen ihren Umgang mit personenbezogenen Informationen für die Nutzer transparent machen. Dies bedeutet unter anderem die Veröffentlichung einer klaren und aussagekräftigen Datenschutzerklärung. Besondere Aufmerksamkeit sollte der Information der Betroffenen über Aspekte der Telemedizin gewidmet werden, die von der normalen „face-to-face“-Medizin abweichen. Idealerweise sollte die Einhaltung der Datenschutzerklärung verifiziert werden können (z. B. durch periodische Auditierung oder durch ein Gütesiegelprogramm).

2. Internet-basierte Angebote zur Telemedizin sollten keine personenbezogenen Daten von den Nutzern durch aktive Elemente oder Cookies heimlich erheben. Wo das anwendbare Recht die Anwendung aktiver Elemente oder von Cookies erlaubt, sollten diese nur mit der Einwilligung des Betroffenen aktiviert werden und ihre Nutzung sollte für die Betroffenen, die um medizinische Beratung nachsuchen, nicht verpflichtend sein. Jedes Internetangebot zur Telemedizin, das aktive Elemente oder Cookies verwendet, sollte darauf in seiner Datenschutzerklärung hinweisen.

3. Verbindungsdaten, die personenbezogene Daten der Besucher eines Internet-Angebots zur Telemedizin enthalten, sollten nicht an Dritte weitergegeben werden. Insbesondere sollten die erhobenen medizinischen Daten nicht für kommerzielle Zwecke genutzt werden.

4. Traditionelle ethische Verpflichtungen für Ärzte und Gesundheitsdienstleister dürfen durch das Angebot dieser Dienste über das Internet nicht gemindert werden. Standesorganisationen sollten die Ergänzung ihrer ethischen Richtlinien in Erwägung ziehen, um sicherzustellen, dass vorbildliche Praktiken in der neuen Umgebung eingehalten werden.

5. Internet-basierte Angebote zur Telemedizin sollten die anwendbaren Richtlinien zum Verbraucherschutz und professionelle Standards einhalten, um sicherzustellen, dass jegliche personenbezogene Daten, die erhoben, empfangen, genutzt oder übermittelt werden, in fairer Weise verarbeitet werden. Die AMA bietet z. B. wertvolle Richtlinien in Bezug auf den Inhalt von Internet-Angeboten, Werbung, Sponsoring und elektronischen Geschäftsverkehr, die in Betracht gezogen werden sollten.

6. Wirksame Sicherheitsmaßnahmen sollten ergriffen werden, um gespeicherte medizinische Informationen (ebenso wie personenbezogene Daten während der Übertragung) in einem Internet-Angebot zur Telemedizin zu schützen. Solche Maßnahmen sollten Verschlüsselung einschließen.

7. Die Standesorganisationen von Ärzten und ähnlichen Berufsgruppen sollten angemessene Richtlinien verabschieden. Überprüfungsmechanismen (z. B. Gütesiegel) sollten geschaffen werden, um die Umsetzung dieser Empfehlung zu verifizieren.

Working Paper on Web-based Telemedicine

– updated at the 38th meeting on 6–7 September 2005 in Berlin –

Telemedicine is the practice of medicine at a distance. The phrase is broad enough to encompass Australia's Flying Doctor Service, remote video consultation after injuries on oil rigs and a medical advice programme on TV or radio. However, this paper is concerned with web-based health services and their data protection implications.

The American Medical Association has observed that "access to medical information via the Internet has the potential to speed the transformation of the patient physician relationship from that of physician authority ministering advice and treatment to that of shared decision making between patient and physician".[1]

[1] American Medical Association, "Guidelines for Medical and Health Information Sites on the Internet http://www.ama-assn.org/ama/pub/category/1905.html

Others may not be so sanguine. However, the growth in health information sites,[2] on-line support and discussion groups[3] and the electronic transfer of health data over the Internet suggests that the Web will become an integral part of the delivery of health care.

The delivery of health services over the Web currently arises in three main settings:

1. The Web as forum for discussion of health issues

This comprises web-based discussion groups, bulletin boards and mailing lists. Postings can be anonymous and the discussions may or may not be moderated. Information posted on these forums tends to be anecdotal rather than authoritative and does not normally involve the payment of any fee or subscription or the creation of a clinical relationship between poster and browser. On a professional level, there are private discussion groups to which a fee is charged and entry is restricted to some subset of the browsing public, such as doctors.

2. Web-based provision of health services from doctor to patient (e-doctors)

There have been some attempts to replicate the traditional doctor-patient relationship in cyberspace. Patients, who may have identified themselves at some point for billing purposes, submit private queries to doctors describing their symptoms. The doctor, whose name and qualifications are available on the site, may respond via email or secure web transaction, setting out advice and a suggested course of treatment. While a doctor will be unable to "lay hands" on a patient, a visual examination might be possible through use of a webcam (although this is not yet usual). National law will typically require that prescriptions to dispense drugs carry a physician's signature and it may sometimes be unethical to prescribe drugs without personally examining the patient.[4]

3. The web as repository of medical records

Sometimes, as a component of (1) and (2) above, there is an electronic repository of personal health records to which the subjects and their authorised health professional have access.

This paper is concerned with the web-based provision of health services.

---

[2] See www.medscape.com, a portal directed at doctors and interested laypeople.

[3] For a survey of medical Internet use see www.hon.ch/Survey/FebMar2001/survey.html.

[4] Pharmacists can dispense medications so long as they receive a prescription (they do not need to see the subject). For an example of a web-based dispenser, see CyberChemist at www.chemist.co.nz/pm/index.cfm.

A selection of data protection issues in web-based telemedicine

Ethical obligations and legal duties of confidentiality

A well-established component of the normal relationship between physician and patient is confidentiality. Doctor-patient confidentiality imposes obligations on the doctor with regard to the personal information of the patient. If a licensed doctor is involved in the provision of health care then the same ethical constraints apply, regardless of whether the doctor's consulting rooms are real or virtual. However there are issues to consider with regard to the privacy of users of on-line health services.

Issues can arise from the use of any transaction data generated in the course of interactions between doctor and patient. Transaction data can under certain circumstances be associated with other web use sessions and with individually identifying data. Prescription data is, for instance, of interest to drug companies. Another concern is basic trust. Users need to be satisfied that a website is a trustworthy repository for their medical information.

If websites of this nature are to succeed, the Web must first be considered an acceptable avenue for the delivery of heath services. Privacy is one of the primary consumer concerns with regard to e-commerce, and the sensitive nature of health information heightens these concerns. Some attempts have been made to promote good practice and thereby public trust. An example is the Health On-Line Code of Conduct which requires that websites `honour or exceed the legal requirements of medical/health information privacy that apply in the country and state where the Web site and mirror sites are located'.[5] Another is the AMA Guidelines for Medical and Health Information Sites on the Internet.[6] Such initiatives are sometimes backed up by self-regulatory web privacy seal programmes with external accreditation and complaints processes.

Collection use and disclosure

Data collection during a telemedical consultation can take place indirectly and even "invisibly", unlike in a physical consultation. Websites often post privacy policies that state what data will be collected,[7] but these rarely cover the use of third party cookies placed by advertising companies. The secondary use of transactional data, especially if combined with other personal data, would be of significant concern.**.** It is unlikely that issues surrounding transactional data or cookies

[5] Available at www.hon.ch. An article in the Journal of Medical Internet Research critiquing that code appears at: www.jmir.org/2000/l/37.

[6] See footnote 1.

[7] For a study suggesting that there is an inconsistency between the privacy policies posted on health web sites and their actual practices, see ehealth.chcf.org/view.cfm?itemID=12497

will be well addressed by conventional ethical rules. This may be compounded by a close partnership that may exist between medical practitioners and drug companies.

Ethical and privacy issues can also arise if transactional data is combined with identifiable patient information for the purposes of research.

Accuracy

There may be aspects of medical advice for which web-based applications will be inappropriate for the foreseeable future. For example, where diagnosis cannot safely be undertaken without more complete information than can be supplied by the subject (although the "second opinion" function will be possible so long as an examining doctor has already accurately recorded symptoms and conditions).

Security

There are security issues in the storage of medical data so that it can be accessed by doctors and patients over the web. TCP/IP is an inherently insecure medium,[8] and methods to remedy this insecurity require effort and expenditure by the website holding the data. While the storage of medical information on-line makes good use of the Web's global ubiquity, it also raises the possibility that remote access may take place from insecure locations such as Internet cafes.

The confidentiality of medical information is valued very highly by consumers, and strong security against unauthorised access would be an essential method of avoiding a breach of confidentiality. It may also be a popular selling point of any telemedicine website.

Positive benefits

Unsurprisingly, this paper has concentrated on areas of concern. Before concluding, it is worth noting aspects of web-based telemedicine which may enhance privacy:

- individuals may be empowered to access information, both their own personal medical records and health care advice, at virtually any time and any place in the world;

- web-based telemedicine provides an impersonal means by which to obtain a "second opinion" – some individuals have felt inhibited and embarrassed to request a second opinion in the traditional manner through their own doctor;

[8] For a brief explanation of the reasons behind this see www.itsecurity.com/tutor/tcpip.htm

- cyber-dispensing is a modern equivalent of "mail order" and can diminish individual embarrassment, particularly in small towns, when filling prescriptions for medications to treat sexually transmitted diseases etc.

Recommendations

The sensitivity of personal medical data means that there must be rigorous adherence to data protection and privacy laws by web-based telemedicine providers. Where such laws do not apply, the generally recognised principles of fair information practice should be followed and all collection, use and disclosure of data should be with the informed consent of the subject. In addition to the normal range of privacy and data protection considerations, the following recommendations are made.

1. Web-based telemedicine sites must make their information policies clear to users. Part of this will involve posting a clear and explicit privacy policy. Special attention should be paid to informing individuals about aspects of the practice of telemedicine which may depart from usual face-to-face medicine. Ideally, there should be verification of compliance with published privacy policies (for example through periodic audit or through a web seal programme).

2. Web-based telemedicine sites should not surreptitiously collect personal data from users by use of active elements or cookies. If applicable law allows the placing of active elements or cookies, they should only be activated with the consent of the subject and their use should not be mandatory for individuals seeking medical advice. Any telemedicine website placing active elements or cookies should highlight this in its privacy policy.

3. Transactional data revealing personal data about visitors to telemedicine sites should not be made available to third parties. In particular, medical data collected should not be used for commercial purposes.

4. Traditional ethical obligations upon doctors and health care professionals must not be diminished by reason of the provision of services over the Internet. Professional associations should consider updating their ethical guidelines to ensure that best practice is maintained in the new environment.

5. Web-based telemedicine sites should comply with applicable guidelines on consumer protection and professional standards so as to ensure that any personal data collected, obtained, used or disclosed are fairly processed. For example, the AMA provides valuable guidelines for website content, advertising and sponsorship and e-commerce, each of which ought to be considered.

6. Strong security measures should be taken to protect any stored medical data on a telemedicine site (as well as personal data in transit). Such measures should include encryption.

7. The associations representing doctors and similar professionals should adopt appropriate guidelines. Auditing procedures (e.g. web seals) should be in place to verify the implementation of these recommendations.

2003

34. Sitzung, 2. und 3. September 2003, Berlin

Arbeitspapier zu potentiellen Datenschutzrisiken im Zusammenhang mit der Einführung des ENUM-Service

Gegenwärtig werden Pilotprojekte zur Einführung des sog. ENUM-Service[1] (einem DNS-artigen Protokoll zur Abbildung von Telefonnummern auf URIs) in zahlreichen Ländern weltweit durchgeführt.

Die öffentlich zugänglichen Dokumente über den ENUM-Dienst haben zu kritischen Äußerungen durch Regierungsstellen, Bürgerrechtsgruppen und Datenschutzaktivisten aus verschiedenen Ländern geführt.

Einige Aspekte der geplanten Struktur geben tatsächlich Anlass zu Datenschutzbedenken:

Die Australische Kommunikationsbehörde hat in einem Diskussionspapier darauf hingewiesen, dass „… die Privatsphäre von ENUM-Kunden verletzt würde, wenn eine Einzelperson, die Informationen auf Basis einer zufällig ausgewählten Telefonnummer verlangt, erfolgreich auf alle Kommunikationsdienste, die mit dieser Telefonnummer verbunden sind (z. B. E-Mail-Adresse, Faxnummer, Handynummer, Festnetztelefonnummer etc.) zugreifen könnte. Diese Information kann dann zur Versendung unverlangter Werbung genutzt werden oder dazu, die Identität eines anderen für kommerzielle oder kriminelle Zwecke vorzutäuschen.“[2]

[1] Siehe z. B. http://www.ENUM.org oder http://www.enum-forum.org für weitere Informationen.

[2] Vgl. Australien Communications Authority: Introduction of ENUM in Australia. Discussion Paper. September 2002, S. 8 (http://www.aca.gov.au/committee/nsg2/ENUM.pdf)

Veröffentlichungen über andere ENUM-Pilotprojekte legen nahe, dass weitere verfügbare Daten Homepages oder sogar Aufenthaltsinformationen umfassen könnten.

Das Amerikanische Electronic Privacy Information Center (EPIC) hat auf weitere voraussehbare Risiken der Einführung von ENUM hingewiesen: „ENUM ist eine global einzigartige Nummer. Wegen der Bequemlichkeit der Nutzung einer einzigen Nummer zur Kontaktaufnahme mit einer Person könnte ENUM in der ferneren Zukunft jedem Menschen zugewiesen werden. ENUM könnte ein global einzigartiger Identifikator (globally-unique identifier – GUID) zur Kennzeichnung von Menschen werden."[3]

Aus Sicht des Datenschutzes wirft die Nutzung existierender Telefonnummern nach dem Internationalen Nummerierungsplan der ITU eine Reihe von Problemen auf, die, falls sie nicht angemessen behandelt werden, zur Gefährdung der Privatsphäre der Nutzer führen könnten. Die Privatsphäre von ENUM-Nutzern könnte besser geschützt werden, wenn eine Option zur Nutzung pseudonymer Daten als ENUM-„Domainnamen" vorgesehen würde, die nicht mit anderen Kommunikations-Identifikatoren eines Nutzers verbunden sind. Auf jeden Fall sollten die Nutzer die Möglichkeit haben, mehrere ENUM-Identifikatoren zu nutzen.

ENUM würde auch eine „Inverssuche" (d. h. das Auffinden personenbezogener Daten des Inhabers zu einer beliebigen Telefonnummer) ermöglichen, was in einigen Ländern für die bereits existierenden Telefonverzeichnisse entweder illegal oder nur unter bestimmten Bedingungen zulässig ist.[4]

ENUM ist das strukturelle Äquivalent eines Domainnamens im Internet. Die Verarbeitung personenbezogener Daten von Inhabern von Domainnamen – insbesondere deren Veröffentlichung in öffentlich zugänglichen Datenbanken im Internet („WhoIs-services") – hat bereits in der Vergangenheit Anlass zu Datenschutzbedenken gegeben.[5] Es ist daher von großer Bedeutung, dass die personenbezogenen Daten von Nutzern von ENUM-Nummern nur aufgrund der informierten Einwilligung der Nutzer zum öffentlichen Abruf bereitgestellt werden. Die bloße Inanspruchnahme eines bestimmten ENUM-Dienstes sollte nicht als eine solche Einwilligung interpretiert werden.

---

[3] zitiert aus http://www.epic.org/privacy/enum/default.html

[4] Vgl. Stellungnahme 5/2000 der Artikel 29-Datenschutzgruppe zur Nutzung von öffentlichen Verzeichnissen für Invert- oder Multikriterien-Suchdienste (Inverse Verzeichnisse); http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp33/wp33de.pdf

[5] Vgl. den Gemeinsamen Standpunkt zu Datenschutzaspekten bei der Registrierung von Domain-Namen im Internet (Kreta, 4./5. Mai 2000); http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_de.htm

Darüber hinaus ist es notwendig, die rechtmäßige Nutzung und die zulässigen Zwecke für ENUM klar festzulegen sowie die Bedingungen für die Löschung der personenbezogenen Daten von Nutzern, die sich dafür entscheiden, den Dienst zu kündigen.

Es hat den Anschein, dass Aspekte des Datenschutzes bisher von den verschiedenen Teilnehmern von den verschiedenen Instanzen im ENUM-Bereich (ITU, IETF und verschiedene Industriegruppen) nicht umfassend behandelt worden sind. Unabhängig davon nimmt die Arbeitsgruppe zur Kenntnis, dass es eine einheitliche Auffassung in der ENUM-Gemeinschaft zu geben scheint, dass ENUM-Dienste nur auf der Basis der informierten Einwilligung des Nutzers angeboten werden sollen, was aus Sicht des Datenschutzes ein weiterer entscheidender Punkt ist.

Die Arbeitsgruppe fordert die ITU und die IETF sowie die beteiligten Industrievertreter und die zuständigen nationalen Regulierungsgremien auf, dem Datenschutz eine hohe Priorität bei der weiteren Entwicklung des ENUM-Dienstes einzuräumen.

34th meeting, 2nd and 3rd September 2003, Berlin

Working Paper on potential privacy risks associated with the introduction of the ENUM service

At present pilot projects for the introduction of the so-called ENUM service[1] (a DNS-like protocol for mapping telephone numbers to URIs) are being run in many countries around the world.

The publicly available documents on the ENUM service have lead to critical statements by governmental authorities, citizens' rights groups and privacy activists from different countries.

Some aspects of the planned structure indeed give rise to privacy concerns:

The Australian Communications Authority has in a Discussion Paper pointed out that "…the privacy of ENUM subscribers would be compromised if an individual requesting information on a randomly chosen telephone number succeeded in accessing all the communications services associated with that telephone number

[1] See e.g. http://www.ENUM.org or http://www.enum-forum.org for further information.

(such as email address, fax number, mobile number, voicemail number etc.). The information may then be used for spamming or to assume someone else's identity for commercial or criminal purposes[2]. Publications on other ENUM pilot projects suggest that other data available could additionally include home pages and even location information.

The US Electronic Privacy Information Center (EPIC) has pointed to more prospective risks of the introduction of ENUM: "ENUM is a globally-unique number. Because of the convenience of using a single number to contact another person, ENUM may be assigned to all humans at some point in the future. ENUM may become a globally-unique identifier (GUID) used to label humans."[3]

From a privacy point of view the use of the existing telephone numbers according to ITU's international numbering plan raises a number of issues which may lead, if not adequately addressed, to threats to users' privacy. The privacy of ENUM users might be protected better if an option would be provided for pseudonymous data not linked to other communications identifiers of a user to be used as ENUM "domain names". In any case users should have the possibility to have multiple ENUM identifiers.

ENUM would also allow for "reverse lookups" (i.e. finding personal data of the assignee to a given telephone number), which is illegal or subject to certain conditions[4] in some countries for existing electronic telephone directories.

ENUM is the structural equivalent of a domain name in the Internet world. The processing of personal data of registrants of domain names – namely its publishing in publicly accessible databases on the web ("WhoIs-services") has given rise to privacy concerns already in the past[5]. It is therefore essential that personal data of registrants of ENUM numbers are only made available for public access with the informed consent of the user. Merely subscribing to a particular ENUM service should not be interpreted as such consent.

It is also a necessity to clearly establish the lawful uses and purposes admitted for ENUM and the conditions for cancelling the personal data of those who decide to unsubscribe from the service.

---

[2] Australian Communications Authority: Introduction of ENUM in Australia. Discussion Paper. September 2002, p. 8 (http://www.aca.gov.au/committee/nsg2/ENUM.pdf)

[3] quoted from http://www.epic.org/privacy/enum/default.html

[4] cf. Opinion 5/2000 of the Article 29 Working Party on The Use of Public Directories of Reverse or Muti-criteria Searching Services (Reverse Directories) (WP33: 13.07.00); http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp32en.pdf

[5] cf. Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet (Crete, 4/5 May 2000); http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm

It seems that privacy aspects have up to now not been dealt with thoroughly by the different players in the ENUM field (ITU, IETF and various industry groups). Nevertheless the Working Group recognizes there seems to be unanimity in the ENUM community that ENUM services should only be offered based on the informed consent of the user which is another crucial point from a privacy perspective.

The Working Group calls upon ITU and the IETF as well as the industry players involved and the competent national regulatory authorities to give privacy matters a high priority in the further development of the ENUM service.

Arbeitspapier zu Intrusion Detection Systemen (IDS)[1]

Was ist ein IDS?

Intrusion Detection ist der Prozess des Erkennens unberechtigter Nutzung von Systemen und Netzen unter Nutzung spezieller Software und/oder Hardware.

Ein IDS eröffnet die Möglichkeit, in Echtzeit Netzwerk- und Systemaktivitäten zu beobachten, unberechtigte Aktivitäten zu identifizieren und nahezu in Echtzeit darauf zu reagieren. IDS-Produkte bieten auch die Möglichkeit, gegenwärtige Aktivitäten vor dem Hintergrund vergangener Aktivitäten zu analysieren, um Trends und Probleme in größeren Zeiträumen zu erkennen.

Zweck und Vorteile von IDS

Der primäre Zweck der Durchführung von Intrusion Detection ist, Konsequenzen unentdeckten Eindringens verhindern zu helfen. Die Implementierung eines Programms wirksamer Sicherheitskontrollen ist ein effektiver Ausgangspunkt dafür, die unterstützende Sicherheitsinfrastruktur zu schaffen. Die Fähigkeit, einen Eindringversuch oder seine Vorbereitung in Echtzeit zu erkennen, ist ein wichtiger Aspekt von Intrusion Detection. Das Wissen, wann eine Attacke stattfindet, und die Fähigkeit, unmittelbar zu handeln, erhöhen die Wahrscheinlichkeit signifikant, Eindringversuche erfolgreich zu beenden und zu ihrer Quelle zurückzuverfolgen. Echtzeit-Erkennung hängt von der Existenz eines Überwachungssystems ab, das im Hintergrund angesiedelt ist und alle Aktivitäten einschließlich der angeschlossenen Geräte überwacht. Das Überwachungssystem muss in der Lage sein, verschiedene Ereignisse zu interpretieren und tatsächliche Attacken zu diagnostizieren.

[1] Dt.: etwa „Einbruchs-Erkennungssysteme“

Die meisten traditionellen IDS arbeiten entweder nach einem netzwerk- oder einem rechner-basierten Ansatz zur Identifizierung von und zum Schutz gegen Attacken[2]. In beiden Fällen suchen IDS nach „Signaturen" von Attacken,spezifischen Mustern, die normalerweise auf böswillige Absichten oder verdächtige Aktivitäten schließen lassen. Ein wirklich effektives IDS wird beide Methoden anwenden.

Datenschutzprobleme

Da IDS viele Verkehrs- oder Ereignisdaten sammeln und aufzeichnen, die sicherlich auch personenbezogene Daten enthalten, dürften die Datenschutzbedenken auf der Hand liegen.

In diesem Zusammenhang hält es die Arbeitsgruppe für notwendig, die Aufmerksamkeit aller Verantwortlichen für die Entwicklung von IDS auf die folgenden Punkte zu lenken: Die Erkennung und Abwehr von Einbrüchen erfordert bei der Suche nach Angriffs-„Signaturen" oder spezifischen Mustern, die normalerweise auf böswillige oder verdächtige Absichten hindeuten, die Analyse des Netzverkehrs und von Protokollierungsdaten von Betriebssystemen.

Die gesammelten Netzwerkverkehrs- oder Ereignisdaten können personenbezogene Daten enthalten, d. h. Daten, die einer bestimmten Person zugeordnet werden können. Die Geräte- oder IP-Adresse kann ein Beispiel eines solchen Datums sein. Daher könnte Intrusion Detection als ein Instrument zur Überwachung von Nutzern und ihrem Verhalten genutzt werden. Wenn Intrusion Detection genutzt werden soll, um „interne" Eindringlinge, d. h. Mitarbeiter einer Organisation, zu erkennen, müssen die Auswirklungen bedacht werden.

Drei Prinzipien, die die Herausforderung für den Datenschutz darstellen, sollten beim Einsatz von Intrusion Detection berücksichtigt werden:

- Intrusion Detection muss dem Zweck der Datensicherheit oder des Systemschutzes dienen,

- die Speicherung der Daten (Netzwerk-Pakete, Audit-Logs) muss dem Schutzzweck angemessen sein,

- eine Festlegung (policy), die die Anforderungen an den Schutz personenbezogener Daten abdeckt, die in IDS gespeichert werden, sollte entwickelt und angewandt werden.

[2] Siehe den technischen Anhang für weitere Informationen.

Der erste Aspekt betrifft die Vereinbarkeit der Überwachung des Verhaltens von Nutzern/Beschäftigten mit Zielen der Intrusion Detection.

Der zweite Aspekt betont, dass nur solche Daten gesammelt und analysiert werden sollten, die zur Erkennung von Attacken erforderlich sind. Nach dem Vergleich von Ereignisdaten mit Angriffs-„Signaturen" des IDS sollten Daten, die nicht länger benötigt werden oder für die kein Hinweis auf einen Angriff bestand, gelöscht werden; die relevanten Daten, die auf einen Angriff hindeuten, sollten in sicherer Weise gespeichert werden. Allerdings kann die Löschung der Daten unter bestimmten Umständen nicht angemessen sein; Ereignisdaten könnten für eine spätere Untersuchung archiviert werden müssen, z. B. zum Zwecke der Rückverfolgung zum Angreifer oder für die spätere forensische Analyse. Einige Daten mögen zunächst unbedenklich erscheinen. Nach weiterer Analyse könnte sich herausstellen, dass sie mit einer Attacke zusammenhängen. Die Korrelation mit später erhobenen Daten könnte auch den Zusammenhang mit einer Attacke beweisen. In jedem Fall und aus verschiedenen Gründen einschließlich des Datenschutzes sollten die Daten umfassend gegen unberechtigte Zugriffe geschützt werden. Die getroffenen Maßnahmen sollten mit der Sicherheitspolitik der Organisation im Einklang stehen.

Der dritte Punkt bedeutet, dass die Vertraulichkeit personenbezogener Daten geschützt und im Einklang mit der generellen Datenschutzpolitik einer Organisation oder mit Rechtsvorschriften, die auf sensible personenbezogene Daten anzuwenden sind, praktiziert werden muss.

Gegenwärtig existieren nur sehr wenige spezielle gesetzliche und regulatorische Anforderungen im Zusammenhang mit Intrusion Detection. Es wird erwartet, dass Gesetze oder Regelungen sich herausbilden, die für einen adäquaten Schutz der Privatsphäre von Individuen sorgen und gleichzeitig IDS und damit zusammenhängenden Aufzeichnungen über Ereignisse erlauben, hinreichend viele Daten zu speichern und zu nutzen, um potentiell schädliche Einbrüche zu erkennen. Bereits jetzt enthalten einige nationale Regelungen das Kriterium der Angemessenheit und der Zweckbestimmung der Nutzung personenbezogener Daten. Einige Länder verfügen über Regelungen hinsichtlich des Schutzes personenbezogener Daten von Arbeitnehmern und von Rechten der Arbeitnehmer, am Schutz ihrer personenbezogenen Daten mitzuwirken. Zusätzlich können verschiedene nationale Regelungen und Verträge über grenzüberschreitende Datenflüsse Intrusion Detection und Datenschutz beeinflussen.

Einige nationale Gesetze und Regelungen verlangen, dass, falls die Überwachung von Aktivitäten von Einzelpersonen stattfindet, z. B. durch Ereignisaufzeichnung und IDS-spezifische Sensoren oder Überwachungsagenten, Arbeitnehmer und Vertragsnehmer in besonderer Weise darüber informiert werden und dies bestätigt haben müssen, bevor solche Maßnahmen ergriffen werden. Dies könnte in der

Form unterschriebener arbeitsvertraglicher Regelungen oder einem gesonderten Schreiben oder jeglichem anderen Weg erfolgen, der im Einklang mit der nationalen Gesetzgebung steht.

Die Grundbegriffe dieser Erwägungen, die den Datenschutz betreffen, sind bereits von einigen Datenschutzbehörden formuliert[3] und insbesondere in dem geänderten Entwurfstext des folgenden Entwurfs für einen Standard integriert worden:

- ISO/IEC WD 18043, „Richtlinien für die Herstellung, den Betrieb und die Verwaltung von Intrusion-Detection-Systemen (IDS)".

Im Hinblick auf die gegenwärtigen Entwicklungen im Zusammenhang mit der Stardardisierung unterstützt die Arbeitsgruppe in vollem Umfang die Integration der oben genannten Erwägungen in alle internationalen, regionalen und nationalen Standards, die die oben erwähnten Angelegenheiten des Datenschutzes betreffen.

Technischer Anhang

Prinzipielle Typen von IDS

Rechner-basierte IDS

Rechner-basierte Intrusion Detection begann in den frühen 80er Jahren, bevor Netzwerke so vorherrschten und so komplex und miteinander verbunden waren, wie sie es heute sind. In dieser einfachen Umgebung war es eine gängige Praxis, Protokolldateien nach verdächtigen Aktivitäten zu durchsuchen.

Rechner-basierte IDS nutzen nach wie vor Protokolldaten, tun dies aber stärker automatisiert und haben sich zu durchdachteren und reaktionsschnellen Erkennungstechniken entwickelt. Rechner-basierte IDS überwachen typischerweise Systeme, Ereignisse und Protokolldateien. Wenn eine dieser Dateien verändert wird, vergleicht das IDS den neuen Eintrag mit Angriffs-„Signaturen", um Übereinstimmungen herauszufinden. In diesem Fall antwortet das System mit der Alarmierung von Systemverwaltern und anderen Hinweisen auf Handlungsbedarf. Es überwacht Dateien im System im Hinblick auf Veränderungen. Der primäre Zweck Rechner-basierter IDS besteht in der Überwachung von Systemen hinsichtlich einzelner Dateiveränderungen.

[3] Die belgische Datenschutzbehörde ist in dieser Hinsicht besonders aktiv gewesen.

Rechner-basierte IDS sind um andere Technologien erweitert worden. Bei einer gängigen Methode zur Erkennung von Einbrüchen werden wichtige Systemdateien und ausführbare Dateien durch Checksummen in regelmäßigen Abständen auf unerwartete Veränderungen überprüft. Die Reaktionszeit hängt direkt von der Frequenz der Kontrollinterwalle ab. Schließlich überwachen einige Produkte Port-Aktivitäten und alarmieren Administratoren, wenn auf bestimmte Ports zugegriffen wird. Diese Art der Kennung integriert ein grundlegendes Maß Netzwerk-basierter Intrusion Detection in die Rechner-basierte Umgebung.

Netzwerk-basierte IDS

Netzwerk-basierte IDS nutzen „rohe" Netzwerkpakete als Datenquelle. Typischerweise benutzen Netzwerk-basierte IDS Adapter, die im „Promiscuous Mode" angewandt werden, zur Überwachung und Analyse des Netzwerkverkehrs in Echtzeit. Der „Promiscuous Mode" macht es für einen Angreifer extrem schwer, die Überwachungsmaßnahme zu erkennen und zu lokalisieren.

Die Funktionalität zur Angriffserkennung benutzt drei gebräuchliche Techniken, um die Signatur einer Attacke zu erkennen:

- Statistische Erkennung von Anomalien

  Im Anomalieerkennungs-Modell erkennt das IDS ein Eindringen, indem es nach Aktivitäten sucht, die von dem normalen Verhalten eines Nutzers oder eines Systems abweichen. Anomalie-basierte IDS erkennen Grundregeln normalen Verhaltens durch Profilbildung für einzelne Nutzer oder Netzwerkverbindungen und durch die Überwachung von Aktivitäten, die davon abweichen.

- Muster-, Befehls- oder Byte-Code-Vergleich

  Die Mehrzahl der kommerziellen Produkte basiert auf Verkehrsanalysen, in denen nach dokumentierten Mustern von Angriffen gesucht wird. Dies bedeutet, dass das IDS programmiert wird, jede bekannte Exploit-Technik zu identifizieren. Dies kann so einfach wie ein Vergleich von Mustern ausgestaltet sein. Das klassische Beispiel besteht darin, jedes Muster in einem Netzwerksegment nach einem definierten Aktivitätsmuster zu durchsuchen, das auf einen Versuch hinweist, auf ein gefährdetes Skript auf einem Webserver zuzugreifen. Einige IDS bauen auf großen Datenbanken auf, die Tausende solcher Muster enthalten. Das IDS überwacht jedes Paket auf der Suche nach Paketen, die eines dieser definierten Muster enthalten.

- Zusammenschau mit weniger gravierenden Vorfällen

Working Paper on Intrusion Detection systems (IDS)

What is an IDS?

Intrusion detection is the process of detecting unauthorized use of systems and networks through the use of specialized software and/or hardware.

An IDS provides the ability to view network and system activity in real time, identify unauthorized activity and provide a nearly real-time automated response. IDS products also provide the ability to analyze today's activity in view of yesterday's activity to identify larger trends and problems.

Purpose and Benefits of IDS

The primary purpose of performing intrusion detection is to help to prevent the consequences caused by intrusions if undetected. Implementing a program of effective security controls is an effective starting point for establishing the supporting security infrastructure. Being able to detect an intrusion attempt or its preparation in real time is an important aspect of intrusion detection. Knowing when an attack is in progress and being able to take immediate action significantly improves the odds of successfully terminating intrusions and tracing intrusion attempts to their source. Real time detection depends upon having a watchdog system that sits in the background and monitors all activities involving the connected devices. The monitoring system must be able to interpret various incidents and diagnose actual attacks.

Most traditional IDS take either a network or a host-based approach to identifying and protecting against attacks[1]. In either case, IDS look for attack signatures, specific patterns that ordinarily indicate malicious intent or suspicious activity. A truly effective IDS will employ both methods.

Privacy concerns

IDS gathering and logging lot of traffic or event data containing certainly some personal data, the privacy concerns seem to be evident.

In this context, the Working Group deems it necessary to draw the attention of all the actors responsible in the implementation of the IDS about the following issues:

[1] See technical annex for details

Recognizing or deflecting intrusions requires the analysis of network traffic and/or audit trails of operating systems while looking for attack signatures or specific patterns that usually indicate malicious or suspicious intent.

Collected network traffic or event data may contain some personal data, i.e., data that can be related to a specific person. The hardware or IP-address may be one example of such a datum. Thus, intrusion detection could be used as an instrument for monitoring users and their behavior. If intrusion detection is to be applied for detecting "internal" intruders, i.e., organizational employees, one must consider the implications.

Three principles that reflect the privacy challenges should be addressed if intrusion detection is employed:

- intrusion detection has to serve the purpose of data or system protection,
- the data collection (network packets, audit logs) has to be adequate to the purpose of protection,
- a policy covering requirements to protect the privacy of personal information collected in IDS should be developed and applied.

As to the first aspect, it questions the conditions of compatibility of supervision of the behaviour of users/employees with intrusion detection objectives.

The second aspect points out that only those data should be gathered and analyzed which are necessary to recognize attacks. After the comparison of event data with the attack signatures of the IDS, data that is no longer needed or with which there has been no indication of an attack should be deleted; the relevant data, which indicate an attack, should be stored in a secure way. However, deleting the data may not be adequate in some instances; event data may need to be archived for later inspection, e.g., for purposes of traceability to the attacker or for forensic analysis at a later date. Some data may at first appear to be benign. After further analysis it may prove to be related to an attack. Correlation with data collected later may also prove it to be related to an attack. In any event and for different reasons including privacy, the data should be strongly protected from unlawfull access. The actions taken should be consistent with the security policy of the organization.

The third point means that the privacy of personal information needs to be protected and managed in accordance with an organizations overall privacy policy and/or any laws that may apply to sensitive personal information.

At the moment there are very few special legal and regulatory requirements associated with intrusion detection. Laws or regulations are expected to emerge that

provide for adequate privacy protection for individuals while at the same time allowing IDS and associated event logs to collect and use sufficient data to identify potentially damaging intrusions. Already some national regulations contain the criteria of adequacy and the related purpose of the use of personal data. Some nations have regulations concerning the protection of workers' personal data and the right of workers' participation in the privacy of their personal data. In addition, various national regulations and treaties regarding transborder data flow may impact on intrusion detection and privacy.

Some national legislation and regulation requires that if monitoring of the activities of people is to take place, e.g., through event logs and IDS-specific sensors/monitoring agents, then the employees and contractors concerned must be specifically informed of, and acknowledge this before operations commence. This could be in the form of signed contractual terms of employment or a particular paper or any other way in accordance with the national legislation.

The essentials of these considerations addressing privacy issues have already been formulated by some data protection authorities[2] and notably integrated in the draft revised text of the following project of standard.

ISO/IEC WD 18043, "Guidelines for the implementation, operation and management of intrusion detection systems (IDS)"

Considering the present developments in the standardisation context, the Working Group fully supports the integration of the above considerations in all international, regional and national standards affecting the above mentioned privacy issues.

Technical annex

The principal types of IDS

Host-based IDS

Host-based intrusion detection started in the early 1980s before networks were as prevalent, complex and interconnected as they are today. In this simpler environment, it was common practice to review audit trail logs for suspicious activity.

Host-based IDS still use audit trail logs, but they are much more automated, having evolved to include more sophisticated and responsive detection techniques. Host-based IDS typically monitor systems, events and security logs on. When

[2] The Belgian Data protection Authority has been specially active with this regard.

any of these files change, the IDS compares the new log with attack signatures to determine if there are any matches. If so, the system responds with administrator alerts and other calls to action. It monitors files on systems for changes. The primary host-based IDS purpose is to monitor systems for individual file changes.

Host-based IDS have expanded to include other technologies. One popular method of detecting intrusions checks key system files and executables via checksums at regular intervals for unexpected changes. The timeliness of response is directly related to the frequency of the polling interval. Finally, some products monitor port activity and alert administrators when specific ports are accessed. This type of detection brings an elementary level of network-based intrusion detection into the host-based environment.

Network based IDS

Network-based IDS use raw network packets as the data source.

Network-based IDS typically utilize network adapters running in promiscuous mode to monitor and analyze network traffic in real time. Promiscuous mode makes it extremely difficult for an attacker to detect and locate.

Attack recognition functionality uses three common techniques to recognize an attack signature:

- Statistical anomaly detection

  In the anomaly detection model the IDS detects intrusions by looking for activity that is different from a user's or system's normal behavior. Anomaly-based IDS establish baselines of normal behavior by profiling particular users or network connections and then monitoring for activities which deviate from the baseline.

- Pattern, expression or byte code matching

  The majority of commercial products are based upon examining traffic looking for documented patterns of attack. This means that the IDS is programmed to identify each known exploit technique. This can be as simple as a pattern match. The classic example is to examine every pattern on the network segment for a defined pattern of activity that indicates an attempt to access a vulnerable script on a web server. Some IDS are built from large databases that contain thousands of such patterns. The IDS monitors every packet, looking for packets that contain one of these defined patterns.

- Correlation of lesser events

2004

35. Sitzung, 14. und 15. April 2004, Buenos Aires, Argentinien

Arbeitspapier zu Datenschutz bei der Verarbeitung von Bildern und Tönen in Multimedia Messaging Services

Mobiltelefone und Fotohandys der neuen Generation werden schnell zu etwas Alltäglichem, was teilweise auch auf die ständig verbesserte Bildqualität zurückzuführen ist.

Obgleich die diesen Geräten zugrundeliegende Technologie sich nicht wesentlich von derjenigen unterscheidet, die etwa in Standardkameras implementiert ist und daher die relevanten rechtlichen Probleme im Prinzip die selben sind, bedingt es besonders die Portabilität und der diskrete Charakter von Kamerahandys, auch in Verbindung mit der Möglichkeit zur Aufnahme von Tönen, dass sie eingesetzt werden können, ohne dass der Fotografierte selbst dies bemerkt.

Dieser Umstand bringt erhöhte Risiken nicht nur für die Privatsphäre des Einzelnen mit sich, sondern kann auch zur Verletzung von Betriebs- und Geschäftsgeheimnissen führen. Tatsächlich wurden bereits Nutzungsverbote für Kamerahandys bestimmte Geschäftsräume betreffend und/oder innerhalb von Fabriken und Arbeitsstätten ausgesprochen.[1]

Es muss betont werden, dass diese Art der Verarbeitung unter den Anwendungsbereich von Strafvorschriften (z. B. Verbreitung jugendgefährdender Schriften) und zivilrechtlichen Regelungen (z. B. Schutz des Rechtes am eigenen Bild, Urheberrechte) fallen kann.

Bild- und Tondateien können personenbezogene Daten, einschließlich sensitiver Daten, enthalten, soweit sie sich auf bestimmte oder bestimmbare natürliche Personen beziehen. In diesem Fall muss berücksichtigt werden, welche Datenschutzprinzipien, insbesondere das Erfordernis nach Information und Einwilligung, Anwendung finden; es sei denn die Datenverarbeitung wird ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten vorgenommen.[2]

---

[1] Siehe hierzu ITU, "Social and Human Considerations for a More Mobile World – Background Paper", Februar 2004, verfügbar unter http://www.itu.int/osg/spu/ni/futuremobile/SocialconsiderationsBP.pdf, S. 17.

[2] Siehe die Entschließungen einiger europäischer Datenschutzbehörden (Italien, 12. März 2003; Ungang, Dezember 2003). Siehe auch das Informationspapier 05.03, Mobile phones with cameras, veröffentlicht vom Office of the Victorian Privacy Commissioner, Australia, verfügbar unter http://www.privacy.vic.gov.au.

Im Hinblick sowohl auf die oben stehenden Erwägungen als auch auf die besonderen Schwierigkeiten bei der Durchsetzung in diesem Gebiet bedingt durch die oben angesprochenen Grundeigenschaften der involvierten Technik (Schnelligkeit, Digitalisierung, leichte Benutzung) möchte die Arbeitsgruppe die Aufmerksamkeit aller betroffenen Unternehmen auf die Notwendigkeit eines erhöhten öffentlichen Bewusstseins für die Datenschutzrisiken lenken, die der Gebrauch von Fotohandys mit sich bringt.

Um diese Ziel zu erreichen, empfiehlt die Arbeitsgruppe eine Reihe von Handlungsoptionen:

– Verbesserung der Aufklärung der Nutzer, wobei besonders ihrem Alter und ihrer Unerfahrenheit Rechnung getragen werden sollte;

– Verbesserung der Informationen durch die Hersteller über den angemessenen Umgang mit Fotohandys;

– Implementierung von technischen Vorkehrungen zur Vereinfachung der Anwendung der relevanten Datenschutzprinzipien und zur Steigerung des Bewusstseins. Mögliche Mittel zur Erreichung dieses Ziels könnten ein Tonsignal[3] sein, das ausgelöst wird, wenn die Fotografierfunktion in Betrieb ist, sowie die Entwicklung von Technologien, die es erlauben, die Fotografierfunktion in gekennzeichneten Bereichen („sicherer Hafen", z. B. Fitnesscenter) abzuschalten.[4]

35th meeting, 14th and 15th April 2004, Buenos Aires, Argentina

Working paper on Privacy and processing of images and sounds by multimedia messaging services

New generation mobile phones and camera phones are rapidly becoming commonplace, partly on account of their ever improving image quality.

Although the technology underlying these devices is not basically different from that implemented, for instance, in standard cameras, and therefore the relevant

[3] Dies ist in Japan auf der Basis einer Selbstregulierung der Industrie bereits umgesetzt während in Südkorea im November 2003 ein Gesetzesvorhaben verabschiedet wurde, das ein aktiviertes Tonsignal mit einer Stärke von mindestens 65 decibel für Fotohandys, unabhängig von deren Einstellungen, fordert.

[4] Siehe ITU, a.a.O, S. 18.

legal issues are in principle the same, the portability and discreet nature of camera phones, also in connection with the possibility of recording sounds, make them especially liable to being used without the photographed being aware.

This circumstance carries enhanced risks as regards not only the privacy of individuals, but also the possible breach of industrial and commercial secrecy. Indeed, a ban on the use of camera phone has been issued with regard to certain premises and/or areas inside factories and workplaces.[1]

It should be pointed out that this type of processing may fall within the scope of provisions related to criminal (e.g., dissemination of obscene materials) and civil law (e.g., protection of a person's rights to his/her own image, copyright issues).

Images and sounds may contain personal data, including sensitive data, insofar as they are related to identified or identifiable natural persons. In this case it has to be considered, which data principles apply, in particular the need for an information notice and consent, except where it is for purely personal or household activity.[2]

In the light of the above considerations as well as of the specific difficulties related to enforcement in this sector on account of the basic features of the technology involved (quickness, digitalisation, easy of use) which were referred to above, the working group would like to draw the attention of all the entities concerned to the advisability of enhancing public awareness on the risks for privacy implied in the use of camera phones.

In order to achieve this end, the Working Group recommends a number of options:

– Improvement of education of the users, particularly taking into account their youth and inexperience;

– improvement of the information given by manufacturers about the appropriate use of camera phones;

– implementation of technological supports to facilitate application of the relevant principles of data protection and enhance awareness. Possible means to

[1] As for these considerations, see ITU, "Social and Human Considerations for a More Mobile World – Background Paper", February 2004, available at http://www.itu.int/osg/spu/ni/futuremobile/SocialconsiderationsBP.pdf , p 17.

[2] See the decisions issued by some European data protection authorities (Italy, 12th March 2003; Hungary, December 2003). See also the Information Sheet 05.03, Mobile phones with cameras, published by the Office of the Victorian Privacy Commissioner, Australia, available at http://www.privacy.vic.gov.au.

achieve this target might include the issue of a sound signal[3] whenever the camera function is operated and developing technologies allowing the camera function to be disabled in certain marked area ("safe havens", e.g. health club)[4].

Arbeitspapier zu einem zukünftigen ISO Datenschutzstandard

Die Arbeitsgruppe begrüßt die Initiativen zur Annahme eines Rahmenstandards zum Datenschutz und zur Einrichtung einer Arbeitsgruppe für Datenschutztechnologie, die gegenwärtig bei der Internationalen Standardisierungsorganisation (ISO) beraten werden. Ein globaler Datenschutzstandard könnte dazu beitragen, die Datenschutzgarantien insbesondere in den Ländern zu schaffen oder zu verbessern, die bisher keinerlei angemessene Datenschutzgesetzgebung aufweisen. Die Standardisierung von Datenschutztechnologie könnte eine wichtige Rolle spielen, wenn es darum geht, Datenverarbeiter bei der Umsetzung nationaler und internationaler rechtlicher Vorschriften zum Datenschutz zu unterstützen.

Technische Standards zu Datenschutz und Technologie bedürfen der eingehenden Diskussion. Die schnelle Annahme eines globalen Standards liegt möglicherweise nicht im langfristigen Interesse der internationalen Gemeinschaft.

Deshalb fordert die Arbeitsgruppe die nationalen Datenschutzbehörden auf, Empfehlungen an die nationalen Standardisierungsgremien zu richten, um technische Normen zu verabschieden, die mit dem rechtlichen Rahmen zum Datenschutz übereinstimmen.

Um größtmögliche Transparenz und Sicherheit für die Datenverarbeiter (Unternehmen und Behörden) zu gewährleisten, die einen zukünftigen Standard umsetzen wollen, betont die Arbeitsgruppe, dass die Befolgung eines technischen Standards nicht notwendigerweise die Befolgung von Rechtsnormen impliziert oder ersetzt.

[3] This is already the case in Japan based on industry self regulation whilst in South Korea legislation was passed in November 2003 requiring at least 65-decibel beeping to be activated on camera phones independently of the settings.

[4] See ITU, Id., p.18.

Working Paper on a future ISO privacy standard

The Working Group takes note and welcomes the initiatives at present under consideration at the International Organisation for Standardisation (ISO) to approve a Privacy Framework Standard and to set up a Study Group on Privacy Technology. A global privacy standard could contribute to create and improve the guarantees on personal data protection particularly in those countries without any kind of adequate regulation. The standardisation of privacy technology could play an important role in assisting controllers to comply with existing national and international legal requirements on data protection.

Technical standards on privacy protection and technology need thorough discussion. A rapid adoption of a global standard may not be in the long-term interest of the international community.

To this effect the Working Group calls on the national Data Protection Authorities to address recommendations to the national standards bodies to approve technical rules that are in line with the legal framework on data protection.

In order to guarantee the highest level of transparency and security to the data controllers (companies and public agencies) which want to implement any future standard the Working Group emphasises that compliance with a technical standard does not necessarily imply or replace compliance with legal regulations.

Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke Allgemeine Empfehlungen

Drahtlose Kommunikation bietet zahlreiche Vorteile wie Portabilität und Flexibilität, erhöhte Produktivität und niedrigere Installationskosten und wird zunehmend populärer. Drahtlose Technologie deckt eine breite Auswahl an unterschiedlichen Fähigkeiten ab, ausgerichtet auf verschiedene Anwendungen und Bedürfnisse. Vorrichtungen drahtloser lokaler Netzwerke (Wireless local area network – WLAN) erlauben den Nutzern zum Beispiel, ihre Laptops von einer Stelle zur anderen innerhalb ihres Büros oder zu Hause zu bewegen, ohne dass dafür Kabel notwendig wären und ohne dass die Netzwerkverbindung verloren geht.

Ad hoc Netzwerke, wie solche, die durch Bluetooth ermöglicht werden, erlauben den Datenabgleich mit Netzwerksystemen, die Anwendungsteilung zwischen

verschiedenen Geräten und beseitigen die Notwendigkeit von Druckerkabeln und sonstigen Verbindungen zu Zusatzgeräten. Mobile Endgeräte wie Personal Digital Assistants (PDA) und Mobiltelefone erlauben Außendienstmitarbeitern den Abgleich von persönlichen Datenbanken und liefern den Zugang zu betrieblich bereitgestellten Diensten wie E-Mail und Internet. Drahtlose Technologie stellt für die Zukunft eine größere Funktionalität in Aussicht.

Dennoch gibt es Risiken bei der Nutzung von drahtloser Technologie, insbesondere weil das der Technik zugrundeliegende Kommunikationsmedium, die Funkverbindung, offen ist für Angriffe, wenn nicht angemessene Sicherheitsvorkehrungen getroffen werden.

Die Risiken umfassen:

– Das Abfangen von Standortdaten und anderen persönlichen Daten über den Netzwerknutzer;

– Unautorisierter und unbemerkter Zugang zu betrieblichen Netzwerken durch externe Nutzer;

– Umgehung von betrieblichen Firewalls und E-Mail-Filterung durch Nutzer drahtloser Netze, die auch Zugang zu Unternehmens- oder Behördennetzen haben, was zu einem Verlust des Schutzes vor Virusattacken und Spam führt;

– Abhören persönlicher Kommunikation und unentdeckte Verbindungen zwischen Nutzern drahtloser Netze, insbesondere auf öffentlichen Plätzen.

Die Arbeitsgruppe fordert sowohl die IEEE Task Group[1] und die WI-FI Alliance[2] als auch die Verkäufer von Produkten der drahtlosen Technologie auf, der Datensicherheit und dem Datenschutz einen hohen Stellenwert bei der gegenwärtigen und zukünftigen Entwicklung von drahtlosen Technologien einzuräumen[3].

---

[1] IEEE 802.11 Working Group for Wireless Area Networks (WLANs). http://grouper.ieee.org/groups/802/11/. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters IEEE.

[2] Wi-Fi Wireless Fidelity http://www.wi-fi.org/OpenSection/index.asp The Wi-Fi Alliance organization, a nonprofit industry group, promotes the acceptance of 802.11 wireless technology worldwide, and ensures that all Wi-Fi CERTIFIED 802.11-based wireless networking gear works with all other Wi-Fi CERTIFIED equipment of the same frequency band and features.

[3] "NIST Publication 800-48: Wireless Network Security 802.11, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf. NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs.

Empfehlungen

A) Risikoanalyse und gewünschtes Sicherheitsniveau

Betreiber drahtloser Netzwerke[4] sollten sich der technischen und der sicherheitstechnischen Auswirkungen von drahtlosen und mobilen Technologien bewusst sein.

Betreiber drahtloser Netzwerke sollten eine Risikoeinschätzung durchführen und eine Sicherheitspolitik entwickeln bevor sie drahtlose Technik einsetzen, um sicherzustellen, dass sie die Risiken für ihre Informationen, Systemoperationen und die Kontinuität der Operationen überprüft haben, und diese handhaben und entschärfen können.

Nutzern drahtloser Netzwerke sollten die technischen und sicherheitstechnischen Auswirkungen drahtloser und mobiler Technologien bewusst gemacht werden.

In ihrem eigenen Interesse sollten alle Nutzer eine persönliche Risikoeinschätzung durchführen, bevor sie drahtlose Technologie oder Dienste kaufen, benutzen oder betreiben, weil ihre eigenen persönlichen Sicherheitsanforderungen bestimmen welche Produkte oder Dienste in Betracht kommen.

B) Netzwerkparametereinstellungen

Betreiber drahtloser Netzwerke sollten den Einsatz drahtloser Technologie sorgfältig planen und geeignete Parameter an den Geräten setzen, um sowohl die Netzwerkfunktion als auch die Sicherheit der Dienste zu garantieren. Insbesondere sollte der Netzwerkzugang durch hohe Sicherheitsstandards zusätzlich geschützt werden.

Nutzer sollten angeleitet werden und es sollte ihnen bewusst gemacht werden, wie sie ihr drahtloses Gerät konfigurieren müssen, um ein hohes Sicherheitsniveau und Vertraulichkeit herzustellen.

C) Sicherheitsmanagement

Betreiber drahtloser Netzwerke sollten Sicherheitsmaßnahmen einführen und kontrollieren, um die Sicherheit der drahtlosen Netzwerke zu erhalten.

Betreiber drahtloser Netzwerke müssen regelmäßig die inhärenten Sicherheitsmerkmale, wie z. B. die Authentifizierung und Verschlüsselung, die in drahtlosen

[4] Englisch: “network manager” = anyone who wants to deploy and use wireless networks.

Netzwerken existieren überprüfen. Die Authentifizierung ist in drahtlosen Netzwerken besonders wichtig und könnte auf einer strengeren Zugriffskontrolle mit regelmäßigem Wechsel der Passwörter basieren.

Betreiber drahtloser Netzwerke sollen die Nutzer über das Sicherheitsniveau in den Netzwerken und über die verfügbaren Maßnahmen zur Sicherstellung der Vertraulichkeit der Kommunikation informieren.

D) Weitere Erwägungen

Anbieter drahtloser Netzwerke sollten die rechtlichen Anforderungen[5] einhalten, die in den unterschiedlichen Rechtssystemen differieren können.

Die Arbeitsgruppe betont ferner, dass Sicherheitskonzepte für die Nutzer schwer zu verstehen sind. Die praktische Anwendung dürfte selbst für erfahrene IT-Spezialisten schwierig sein. Die Industrie als Ganzes sollte das Problem sowohl auf der technischen als auch auf der Informationsebene angehen, um das Vertrauen in die Technologie zu verbessern. Die Voreinstellungen sollten ein hohes Datenschutzniveau gewährleisten.

Internet-Diensteanbieter, insbesondere Web-Mailer, sollten die Möglichkeit zur Verschlüsselung auf Anwendungsebene bieten. Werden sensitive Daten über drahtlose Netzwerke übertragen ist eine starke Verschlüsselung unverzichtbar.

Nutzer sollten nicht davon abgehalten werden, öffentlich zugängliche Dienste anonym oder unter Pseudonym zu nutzen.

Working Paper on potential privacy risks associated with wireless networks. Main Recommendations.

Wireless communications offer many benefits such as portability and flexibility, increased productivity, and lower installation costs and are becoming increasingly popular. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices or homes without the need for wires and without loosing network connectivity.

[5] Vgl. Art. 4 Richtlinie 2002/58/EC des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems, application sharing between devices and eliminate the need for cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and mobile phones allow remote workers to synchronize personal databases and provide access to corporate services such as e-mail, and Internet access. Wireless technologies offer the prospect of greater functionality in the future.

However, there are risks associated with the use of wireless technology, in particular because the technology's underlying communications medium, the airwave, is open to intrusion unless appropriate security precautions are taken.

These risks include:

– The capture of location data and other personal data about the network user;

– Unauthorised and undetected access to corporate networks by external users;

– Bypassing of corporate firewalls and e-mail filtering by wireless users also connected to corporate networks, leading to loss of protection from virus attack and spam;

– Eavesdropping of personal communications and undetected connections between wireless network users, especially in public places;

The Working Group calls upon the IEEE Task Group[1] and the WI-FI Alliance[2] as well as the vendors involved in wireless products to give data security and privacy matters a high priority in the current and future development of wireless technology[3].

[1] IEEE 802.11 Working Group for Wireless Area Networks (WLANs). http://grouper.ieee.org/groups/802/11/. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters IEEE.

[2] Wi-Fi Wireless Fidelity http://www.wi-fi.org/OpenSection/index.asp The Wi-Fi Alliance organization, a nonprofit industry group, promotes the acceptance of 802.11 wireless technology worldwide, and ensures that all Wi-Fi CERTIFIED 802.11-based wireless networking gear works with all other Wi-Fi CERTIFIED equipment of the same frequency band and features.

[3] "NIST Publication 800-48: Wireless Network Security 802.11, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf [NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs.

Recommendations

A) Risk Analysis and desired Security Level

Wireless network managers[4] should be aware of the technical and security implications of wireless and handheld device technologies.

Wireless network managers should perform a risk assessment and develop a security policy before considering wireless deployment in order to ensure that they have examined and can manage and mitigate the risks to their information, system operations, and continuity of operations.

Wireless network users should be made aware of the technical and security implications of wireless and handheld device technologies.

For their own concerns, all users should perform a personal risk assessment before purchasing, using or running wireless technologies and services, because their own and personal security requirements will determine which products or services should be considered.

B) Network Parameter Settings

Wireless network managers should carefully plan the deployment of wireless technology and set appropriate parameters on devices in order to guarantee both network functionalities and service security. In particular, network access should be covered by high security standards.

Users should be guided and should be made aware of how to configure wireless devices to ensure a high level of security and confidentiality.

C) Security management

Wireless network managers should establish security management practices and controls to maintain the security of the wireless network.

Wireless network managers must routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies. The authentication in wireless network is very important and could be based on a stronger access control with regularly modified passwords.

[4] Anyone who wants to deploy and use wireless networks.

Wireless network managers should inform the user of the level of security of the network and the measures available to safeguard the confidentiality of communication.

D) Other Considerations

Providers of wireless networks should comply with the legal requirements[5] which may differ from one jurisdiction to another.

The Working Group stresses also that security concepts are difficult for users to understand. Practical application may also be difficult even for experienced IT specialists. The industry as a whole should tackle the problem at both technical and informational levels in order to enhance confidence in technology. The default setting should provide for a high level of privacy protection.

Service providers over Internet, in particular WEB mailers, should offer the opportunity for application level encryption. If sensitive data are communicated through wireless networks strong encryption is indispensable.

Users should not be prevented from using pseudonymous or anonymous access to publicly available services.

Arbeitspapier zu Meinungsäußerungsfreiheit und Persönlichkeitsrecht bei Online-Publikationen*

Bedenkt man, dass mehr als 10 Jahre vergangen sind, seit das Internet für Online-Publikationen genutzt wird, ist es notwendig, das Verhältnis zwischen den elementaren Menschenrechten der freien Meinungsäußerung und des Persönlichkeitsrechts erneut zu überdenken. In jüngster Zeit wurde von Personen, die personenbezogene Daten im Internet veröffentlicht haben, geltend gemacht, dass das Recht auf freie Meinungsäußerung ihnen erlaube, das Recht der Betroffenen am Schutz ihrer persönlichen Daten zu übergehen.

[5] See Art. 4 Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

* Aufgrund von Zuständigkeitsproblemen waren Norwegen und Schweden nicht in der Lage, das Dokument zu unterstützen.

Es muss aber betont werden, dass diese genannten Rechte dieselbe Priorität genießen und im allgemeinen keines von beiden dem anderen vorgehen sollte.

Das Datenschutzniveau bei Online-Publikationen sollte sich vielmehr an einem vorsichtig ausgewogenen Kompromiss zwischen dem individuellen Persönlichkeitsrecht und dem Recht auf freie Meinungsäußerung orientieren.

Beziehen sich Informationen über das Privat- oder Familienleben, die private Korrespondenz und die Privatwohnung auf eine bestimmte oder bestimmbare natürliche Person, müssen die zentralen Vorschriften über den Datenschutz Anwendung finden. Das Recht auf freie Meinungsäußerung darf gegenüber dem Persönlichkeitsrecht nicht die Oberhand gewinnen.

Ungeachtet besonderer Privilegien für journalistische Aktivitäten, die gesetzlich geregelt werden können, sollten die folgenden vorrangigen Prinzipien bei Online-Publikationen Beachtung finden:

– Die Daten müssen in legaler und fairer Weise erhoben werden.

– Es muss ein Recht auf Gegendarstellung und auf Berichtigung von unwahren Tatsachen eingeräumt werden.

– Es muss ein Recht auf Zugang zu den veröffentlichten Daten eingeräumt werden.

– Es muss ein Beschwerdeverfahren eingerichtet werden.

Journalisten sind nicht verpflichtet, ihre Informationsquellen zu überprüfen und gegenüber den betroffenen Personen oder anderen offen zu legen, außer in gesetzlich besonders vorgesehenen Fällen.

Working paper on freedom of expression and right to privacy regarding on-line publications[*]

Bearing in mind that over 10 years have passed since the Internet has been used for on-line publication, it is necessary to reconsider the relationship between the fundamental human rights to freedom of expression and to privacy. In recent cases

[*] Regarding their problems of jurisdiction Norway and Sweden were not able to support the document

persons who published personal data on the Internet demanded that right to freedom of expression allows them to neglect the right to privacy of the concerned persons.

It must be emphasized that these rights have equal precedence and in general neither should overrule the other.

The level of personal data protection in on-line documentation should be a carefully balanced compromise between individual right to privacy and the right to freedom of expression.

If the information regarding private and family life, private correspondence, and dwelling relate to an identified or identifiable natural person, the main provisions concerning personal data protection must be applied and in balance. The right to freedom of expression should not prevail over the right to privacy.

Notwithstanding any special privileges for journalistic activities that may be allowed by law, the following overriding principles should continue to apply regarding on-line-publications:

– The data must be collected in a legal and a fair way.

– There must be a right to reply and to rectification of untrue factual information.

– There must be a right to access to published data.

– There should be established a mechanism to deal with complaints.

Journalists are not obliged to check up and disclose to data subject or any other body, the source of information, except in situations provided by law.

36. Sitzung, 18. und 19. November 2004, Berlin

Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs

Wie in der realen Welt besteht Kriminalität zum größten Teil aus Eigentumsdelikten. Die am meisten verbreitete Form sind offenbar Betrug und Urheberrechtsverletzungen.

Das Zentrum für Beschwerden gegen Internetbetrug (Internet Fraud Complaint Center (IFCC)) nennt Internetbetrug in seinem Bericht für 2002 als wachsendes Problem[1]. Betrug bei Versteigerungen war das am häufigsten angezeigte Vergehen.

Der Ministerrat der OECD hat die „OECD Richtlinien zum Schutz der Verbraucher vor betrügerischen grenzüberschreitenden Handelspraktiken am 11. Juni 2003 beschlossen[2]. Viele Mittel wurden zur Bekämpfung der Cyberkriminalität/des Online-Betrugs vorgeschlagen. Die meisten davon betreffen verbesserte Formen der Strafverfolgung und verbesserte Zusammenarbeit zwischen den Regierungen. Auch wenn diese Mittel zweifellos nützlich sind, können sie auch zu Datenerhebungen und -übermittlungen Anlass geben, die Datenschutzprobleme aufwerfen.

Demgegenüber sind Mittel, die die Vorbeugung in den Vordergrund stellen, bisher offenbar weniger beachtet worden. Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation betont die positiven Wirkungen, die präventive Techniken auf die Senkung der Kriminalitätsrate im allgemeinen und die Sicherung von Aspekten des Datenschutzes bei der Strafverfolgung haben können. Die Internationale Arbeitsgruppe zum Datenschutz bei der Telekommunikation hat sich mit diesem Fragenkreis bereits früher befasst[3].

Die folgenden Methoden und Techniken können zur datenschutzgerechten Bekämpfung des Online-Betrugs genutzt werden:

- *Digitale Signaturen* können dazu beitragen, die Geschäftspartner zu identifizieren;

- *Treuhanddienste* können den Austausch von Waren und Geld für beide Parteien durch den Einsatz von vertrauenswürdigen Dritten sicherer machen;

- *Auditierung und Gütesiegel* können den Kunden helfen, vertrauenswürdige Online-Händler zu erkennen;

- *Verbesserte Bezahlverfahren* sind weniger anfällig für Betrugsmanöver;

- *Besser informierte Kunden* werden seltener Opfer solcher Manöver;

---

[1] http://www1.ifccfbi.gov/strategy/wn030409.asp

[2] http://www.oecd.org/dataoecd/24/33/2956464.pdf

[3] Common Position on the detection of fraud in telecommunications adopted at the 27th Meeting of the Working Group on 4-5 May 2000 in Rethymnon / Crete, available online http://www.datenschutz-berlin.de/doc/int/iwgdpt/fr_en.htm

- *Besser informierte Unternehmen* neigen eher dazu, Systeme zu nutzen, die besser gegen Betrug geschützt sind

- *Verbesserte Sicherheit* kann viele Formen betrügerischen Handelns verringern, das Computersysteme ins Visier nimmt oder deren Schwächen ausnutzt, um Menschen zu täuschen.

Die Erläuterungen zu diesem Dokument enthalten praktische Beispiele hierfür.

Schlussfolgerungen

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation empfiehlt, dass Behörden

- in erster Linie Mittel einsetzen sollten, die dem Online-Betrug vorbeugen, bevor sie Maßnahmen ergreifen, die derartige Straftaten nach ihrer Begehung bekämpfen sollen,

- Informationen und Beispiele der datenschutzfreundlichen Bekämpfung von Online-Betrug sammeln sollten,

- solche Informationen austauschen sollten,

- die Annahme datenschutzfreundlichen Verhaltensmaßregeln durch die Wirtschaft, insbesondere die Diensteanbieter, fördern sollten und

- die Öffentlichkeit und die Wirtschaft entsprechend informieren sollten.

Erläuternder Bericht zum Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs

Dieser erläuternde Bericht stellt detaillierter einige der Verfahren zusammen, die genutzt werden können, um Online-Betrug ohne Verletzung von Bürgerrechten zu bekämpfen. In diesem Bericht wird auf vorhandene Beispiele entsprechender Dienstleistungen und Produkte hingewiesen. Dies ist nicht als positive Bewertung durch die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation zu verstehen. Die Beispiele dienen lediglich als Anhaltspunkte für bereits vorhandene Lösungen. Die Informationen und Hyperlinks entsprechen dem Stand vom November 2004.

Digitale Signaturen

Digitale Signaturen können dazu beitragen, die Geschäftspartner zu identifizieren. Eine digitale Signatur ist eine von mehreren Möglichkeiten, um sich der Identität des Geschäftspartners zu vergewissern.

Digitale Signaturen sind nicht überall verfügbar und sie sind nicht perfekt. Es wird immer Mittel geben, um echte, aber irreführende Zertifikate[4] zu erhalten oder um Menschen dazu zu verleiten, ohne digitale Signatur ein Geschäft abzuschließen, aber digitale Signaturen sind dennoch hilfreich.

Unternehmen können signierte Verkaufszertifikate ausstellen, die dem Käufer den Nachweis des Kauf ermöglichen.

Treuhandsysteme

Systeme, in denen der Kaufpreis nicht sofort an den Verkäufer ausgezahlt, sondern von einem vertrauenswürdigen Dritten treuhänderisch verwaltet wird („escrow service" – Treuhanddienst), können Betrug bei der Lieferung verhindern, bei dem ein unehrlicher Verkäufer Vorauszahlung verlangt und dann nicht liefert. Diese Art des Betrugs ist besonders verbreitet bei Online-Auktionen. Der IFCC 2002 Internet Betrugsbericht nennt den Fall „Vereinigte Staaten gegen Teresa Smith", in dem Frau Smith Computer auf Internet-Auktionsplattformen verkaufte, aber nicht lieferte. Sie betrog auf diese Weise mehr als 300 Opfer und erschlich mehr als $ 800.000.

Bei einem Treuhanddienst übergibt der Käufer den Kaufpreis dem Treuhänder. Der Verkäufer erhält eine Information vom Treuhänder, dass das Geld für ihn bereit liegt und nicht zurückgezogen werden kann, während der Käufer den Treuhänder anweist, das Geld auszuzahlen, wenn er den Kaufgegenstand erhalten hat. Im Streitfall bleibt das Geld beim Treuhänder hinterlegt, bis eine Einigung erzielt werden kann. Ein richtig eingesetzter Treuhanddienst kann Online-Betrug erheblich erschweren. Der Betrüger muss den Käufer oder den Treuhänder dazu verleiten, den Kaufpreis zu überweisen (z. B. indem er Gegenstände liefert, die ordnungsgemäß erscheinen, aber qualitativ minderwertig sind, oder indem er eine Auszahlungsanweisung fälscht). Alle diese Manöver sind allerdings für den Betrüger riskant und kostspielig.

Der Nachteil von Treuhanddiensten ist, dass sie für beide Parteien verfügbar und von ihnen akzeptiert sein müssen und dass sie Geld kosten. Personen, die an

[4] Z. B. kann ein Komplize ohne Vorstrafen dafür bezahlt werden, dass er seine Signatur für betrügerische Zwecke „verleiht".

Geschäften mit legitimen, aber anstößigen Produkten (z. B. Pornographie) beteiligt sind, lehnen die Inanspruchnahme eines Treuhanddienstes möglicherweise aus Datenschutzgründen ab. Hochprofessionelle Betrüger können ihre eigenen Treuhanddienste anbieten. Andere Kriminelle können leichtgläubige Menschen davon abhalten, einen Treuhanddienst zu nutzen.

Ein zusätzlicher Vorteil aus Datenschutzsicht besteht darin, dass der Verkäufer vomTreuhänder die Information erhält, dass der vereinbarte Kaufpreis bereitliegt. Der Verkäufer muss nicht die Kreditwürdigkeit des Käufers überprüfen. Er muss nur dem Treuhänder vertrauen.

Ebay, ein populäres Internet-Auktionshaus, empfiehlt Treuhanddienste:
http://www.ebay.com/help/community/escrow.html

Verkäufer sollten ermutigt werden, mit Treuhanddiensten zusammenzuarbeiten und sie ihren Kunden zu empfehlen.

Auditierung und Gütesiegel

Wie kann man sich der Vertrauenswürdigkeit des Verkäufers versichern? Um diese Frage zu beantworten, sind verschiedene Programme für Audits und Gütesiegel entwickelt worden.

Diese Programme mögen nicht perfekt sein, aber sie sind ein Unterscheidungsmerkmal zwischen einem Online-Shop, über den die Kunden keine Informationen haben, und einem Online-Shop, der von einer vertrauenswürdigen Stelle geprüft worden ist.

Verbesserte Bezahlverfahren

Ein großer Teil des Potentials für Missbrauch und Betrug liegt in technischen und organisatorischen Schwächen der Bezahlverfahren. Vor allem Kreditkarten sind besonders leicht zu missbrauchen. Viele Formen des Betrugs beziehen sich auf Kreditkartenzahlungen.

Die Behörden sollten prüfen, was zur Verbesserung der Bezahlungssysteme getan werden kann, so dass Betrüger weniger Möglichkeiten haben, um Sicherheitslücken auszunutzen.

Kundeninformation

Die beste Waffe gegen Betrug ist Information. Viele Länder haben bereits gute Kundeninformationsdienste, andere sollten nachziehen. In einigen Ländern bietet auch die Polizei Informationen an.

Es gibt genug Informationen (allerdings häufig auf Englisch). Die Bereitstellung und Verbreitung solcher Informationen in einer Sprache und Form, die den Bürgern entspricht, kann von großer Hilfe sein.

Informationen für Unternehmen

Sobald die Wirtschaft Systeme mit höherer Sicherheit einsetzt, die weniger anfällig für Manipulationen sind, dürfte dies die Betrugsfälle reduzieren.

Erhöhte Sicherheit

Betrug im Zusammenhang mit Angriffen auf Computersysteme wird häufig erleichtert durch unzureichende Sicherheitsmaßnahmen und unsicheren Programmen.

Betrug, der auf Computersysteme abzielt, ist eine verhältnismäßig neue Kriminalitätsform. Beim Computerbetrug ist das Hauptziel des Betrügers das Computersystem des Opfers. Der Kriminelle ist bestrebt, durch Manipulationen am Computer Zugriff auf finanzielle Mittel, Zugriffsrechte oder Ressourcen zu erhalten, die ihm nicht zugänglich sind oder die ihn Geld kosten würden. Einige Betrüger kopieren Kreditkarten-Daten, um Kreditkarten-Gesellschaften oder Banken zu betrügen[5]. Diese Betrugsart kann den Nutzer einbeziehen, allerdings nur zu einem bestimmten Grad, etwa indem jemand dazu verleitet wird, eine Programm herunterzuladen, das es dem Angreifer erlaubt, auf den Computer zuzugreifen („Trojanisches Pferd“).

Andere Kriminelle fälschen e-mails von Banken, um die Empfänger dazu zu veranlassen, Zugangsdaten für ihre Konten einzugeben (dies wird als „phishing“ bezeichnet). Phisher missbrauchen Sicherheitslücken in Browsern und e-mail-Programmen, um den fälschlichen Eindruck zu erwecken, jemand besuche die Website seiner Bank, während er in Wirklichkeit auf einer gefälschten Seite mit einer anderen Adresse ist.

Eine inzwischen verbreitete Angriffsart ist die heimliche Zweckentfremdung von Computern zur Versendung von unerwünschter Werbung (Spam). Dies ist zwar nicht Betrug im klassischen Sinn, es beruht aber auf Täuschung, um rechtswidrige Handlungen vorzunehmen. Darüber hinaus bieten viele Spam-Versender in betrügerischer Weise Güter und Dienstleistungen an. Weniger Spam bedeutet weniger Betrug.

[5] Dies wird häufig als „Identitätsdiebstahl“ bezeichnet.

Der beste Weg, solche Straftaten zu bekämpfen, ist die Verbesserung der Computersicherheit. Die Behörden können bessere Sicherheitsmaßnahmen, schnellere Reaktionen auf Sicherheitslücken und -bedrohungen und Rechtsbehelfe zum Schutz vor Schäden durch unsichere Systeme vorschlagen. Es ist möglich, die Bürger zum Einsatz von Technologie mit höherer Sicherheit aufzufordern.

Hersteller können dies ebenfalls unterstützen, indem sie die Vorteile von Hard- und Software-Lösungen mit höherer Sicherheit herausstellen, insbesondere beim Einsatz von Firewalls bei Breitbandverbindungen. Diese können die Angriffsmöglichkeiten reduzieren, indem sie unerkannte eingehende Verbindungsversuche blockieren.

Manchmal können sogar einfache Dinge wie ein gutes e-mail-Programm und ein gut gemachter Web-Browser hilfreich sein.

36th meeting, 18th and 19th November 2004, Berlin

Working Paper on Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way

Just like in the offline world, the bulk of online crime is crime against property. The most common forms appear to be fraud and copyright piracy.

The Internet Fraud Complaint Center (IFCC) lists internet fraud as a growing problem in its 2002 report[1]. Auction fraud was the most reported offence.

The OECD Council adopted the "OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders"on 11 June 2003[2].

Many remedies have been suggested to combat cyber-fraud. Most of these involve improved forms of prosecution and better cooperation between governments. Whilst these remedies are no doubt useful, they may also involve data collection and data transfers that raise privacy concerns.

It appears that remedies which emphasize prevention have so far received considerably less attention. The International Working Group on Data Protection in Telecommunications stresses the positive effects that preventive techniques may

[1] http://www1.ifccfbi.gov/strategy/wn030409.asp

[2] http://www.oecd.org/dataoecd/24/33/2956464.pdf

have on the reduction of the crime rate in general and the safeguarding of privacy aspects concerned with prosecution. The International Working Group on Data Protection in Telecommunications has addressed this subject before[3].

The following methods and techniques may be used to combat cyber-fraud in a privacy-friendly way:

- *Digital signatures* can help to identify business partners;
- *Escrow systems* can make the exchange of goods and money safer for both parties through the use of a trustworthy third party;
- *Audits and quality* seals can help customers to recognize trustworthy online stores;
- *Improved payment* systems are less vulnerable to fraud;
- *Better Informed customers* are less likely to become victims of fraud;
- *Better informed businesses* are more likely to employ systems that are better protected against fraud;
- *Enhanced security* can reduce many forms of fraud that target computer systems or exploit their weaknesses to deceive humans.

The explanatory paper to this document contains examples.

Conclusions

The International Working Group on Data Protection in Telecommunications recommends that authorities should

- Promote privacy-friendly means to prevent cyber-fraud before looking at other measures to combat cyber-fraud
- Collect information and examples on privacy-friendly means of combating cyber-fraud; and
- Exchange such information;

[3] Common Position on the detection of fraud in telecommunications adopted at the 27th Meeting of the Working Group on 4–5 May 2000 in Rethymnon / Crete, available online http://www.datenschutz-berlin.de/doc/int/iwgdpt/fr_en.htm

- Promote the adoption of privacy-friendly codes of practice by the business community, especially intermediaries

- Inform the public and the business community.

Explanatory Paper
(To the paper "Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way")

This explanatory paper lists some of the techniques that can be used to combat cyber-fraud in without infringing civil rights in more detail. Throughout this paper, examples for existing services and products have been provided. These are not to be understood as an endorsement by the International Working Group on Data Protection in Telecommunications. They merely serve as a guideline for what is already available. All information and hyperlinks were last checked in November 2004.

Digital Signatures

Digital signatures can help identify business partners. A digital signature is one of the few ways one can be certain of the business partner's identity.

Digital signatures are not available everywhere and not perfect. There will always be means to obtain genuine but misleading certificates[4], or to trick people into doing business without a signature, but it does help.

Companies may issue sales certificates that are signed, thereby giving the buyer proof of the sale as well.

Escrow Systems

Systems where the money is not immediately paid to the seller, but kept by a trustworthy third party ("escrow service") may prevent delivery fraud where a dishonest seller demands advance payment and never delivers. This kind of fraud is especially common in online auctions. The IFCC 2002 Internet Fraud Report lists the case of "United States v. Teresa Smith", in which Mrs. Smith sold computers on internet auction sites but did not deliver. She defrauded more than 300 victims for over $ 800.000.

[4] E.g. it is possible to pay an accomplice with no criminal records to "lend" his signature for the purpose of fraud.

With an escrow system, the buyer gives the money to the escrow service. The seller receives information from the escrow service that the money is ready for him and cannot be withdrawn, while the buyer releases the money only when he receives the goods. In case of dispute, the money remains blocked until a proper decision can be reached. A properly used escrow service can make delivery fraud very impractical. The swindler must deceive the buyer or the escrow service into releasing the money (e.g. by delivering goods that appear legitimate, but are of lower quality, or faking a release order). However, all of these countermeasures appear risky and expensive for the swindler.

The drawback of escrow services is that they must be available and accepted by both parties, and that they cost money. Persons involved in deals with legitimate but embarrassing goods (e.g. pornography) may refuse to use an escrow service for privacy reasons. Highly professional swindlers can offer their own fraudulent escrow service. Other criminals may talk gullible people into not using an escrow service.

As an additional privacy benefit, the seller receives information from the escrow service that the promised money is available. The seller does not need to check the buyers creditworthiness. He merely has to trust the escrow service.

Ebay, a popular online auction house, recommends escrow services:
http://pages.ebay.com/help/community/escrow.html

Sellers should be encouraged to cooperate with good escrow services and recommend them to their customers.

Audits and Quality Seals

How can one know that a seller is trustworthy? To address this question, various programs for audits and quality controls have sprung up.

These programs may not be perfect, but they do make a difference between a web shop customers know nothing about and one that has been examined by a trusted organisation.

Improved Payment Systems

Much of the potential for abuse and fraud lies in technical and organisational weaknesses of payment systems. Credit cards, in particular, have proven to be too easy to abuse. Many forms of fraud involve credit card payments.

The authorities should examine what can be done to improve payment systems so that swindlers have less opportunity to exploit weaknesses.

Customer Information

The best weapon against fraud is information. Many countries already have good consumer information services in place, others should follow suit. In some counties, the police agencies offer information as well.

There is enough information available (though often in English). Creating and spreading such information in a language and form appropriate for the citizens can help a lot.

Information for Businesses

The adoption by business of more secure systems that are less susceptible to compromise should reduce the incidence of fraud.

Enhanced Security

Frauds that attack computer systems frequently profit from inadequate security measures and insecure software.

Fraud targeting computer systems is a completely new form of crime. In computer fraud, the main target of the swindler is the computer system of the victim. The criminal aims to obtain funds, access rights or resources that are either unavailable to him or would cost him money by manipulating a computer. Some swindlers copy personal data to deceive credit card companies or banks[5]. This kind of fraud may involve the user, but only to a limited degree, such as tricking somebody into downloading a program that permits an attacker access to his computer (a "Trojan Horse").

Other criminals forge e-mails from banks to make the recipients enter confidential access information for their bank accounts (this is called "phishing"). Phishers abuse security leaks in web browsers and e-mail software to aid in the deception, e.g. to create the impression that somebody is visiting the web site of his bank while he is actually on a fake page with a different address.

A type of attack that has become common is computer hijacking to send out spam. This is not "fraud" in the classic sense, but it still involves deception to commit illegal actions. Moreover, many spammers sell fraudulent products or services. Less spam means less fraud.

[5] This is often called "identity theft".

The best way to combat such crimes is to improve computer security. The authorities can propose better security measures, quicker responses to leaks and threats as well as legal remedies against damage by insecure systems. It is possible to encourage the use of more secure technology by citizens.

Suppliers can help by promoting the advantages of more secure hardware and software solutions, especially the use of firewalls in conjunction with broadband connections. These can reduce the opportunities for attack by blocking unrecognised inward connection attempts.

Sometimes, even simple things like a good e-mail-program and a well-made web browser can help.

Arbeitspapier zu Lehrplänen zur Internetsicherheit unter Berücksichtigung nationaler, kultureller und rechtlicher (einschließlich datenschutzrechtlicher) Anforderungen

Sicherheit von Informationssystemen

In der frühen Entwicklungszeit der Automation war die Sicherheit von Informationssystemen vor allem mit bescheidenen Stand-alone-Systemen in geschlossenen Netzwerken befasst und war entsprechend in ihrer Reichweite begrenzt auf die Übernahme relativ einfacher Regeln für die physische, hard- und softwaremäßige Sicherheit.

Später haben die starke Zunahme von immer leistungsfähigeren Personalcomputern, die Verbreitung neuer Informations- und Kommunikationstechnologien, der umfassende Gebrauch des Internet und die zunehmende Abhängigkeit menschlicher Aktivitäten von einem ordnungsgemäßen Funktionieren der Informationssysteme die Situation komplexer gemacht.

Heute kann die Sicherheit von Informationssystemen nicht mehr begrenzt werden auf Gegenmaßnahmen gegen Symptome angesichts technischer Sicherheitsbedrohungen, sondern es ist nötig, elementare Änderungen von Verhaltensmustern von allen Beteiligten einzuführen, um den eindringlichen Bedrohungen zu begegnen, denen menschliche Werte und Menschenrechte bezüglich der Sicherheit im Internet ausgesetzt sind.

Dieser neue globale und systematische Zugang zur Informationssicherheit ist unterstrichen und vorangetrieben worden durch die OECD, deren Veröffentlichung „Guidelines for the Security of Information Systems and Networks“ die Notwendigkeit anerkennt, eine echte „Sicherheitskultur“ zu entwickeln.

Sicherheit von Informationssystemen versus Datenschutz

Um ihre jeweiligen Aufgaben zu erfüllen, müssen heute alle Organisationen, gleich ob es öffentliche oder private Stellen sind, eine zunehmende Menge von Daten und immer mehr personenbezogene Daten in ihren Informationssystemen erheben, verarbeiten und speichern.

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht und ein wirksamer Datenschutz kann nicht erreicht werden ohne angemessene Sicherheit. Das ist bereits 1980 durch die „OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” anerkannt worden. Da Sicherheit zwingend erforderlich ist, um Persönlichkeitsrechte zu schützen, verlangt der spezifische gesetzliche Schutz personenbezogener Daten im Vergleich zu anderen Daten und deren Sicherheit oft einen völlig verschiedenen Zugang. Die fundamentalen Datenschutzprinzipien wie das Recht auf Vergessen, das Recht auf Zugang, die Begrenzung der Erhebung und Verarbeitung sowie das Verhältnismäßigkeitsprinzip sind bedauerlicherweise keine grundsätzlichen Prinzipien, die von Sicherheitsexperten notwendigerweise anerkannt werden.

Informationssicherheitsexperten

Heute hat sich die Sicherheit von Informationssystemen nicht nur mit den technischen Risiken der verschiedenen Computerplattformen, Netzwerke, Protokolle oder anderen Bestandteilen von Informationssystemen zu befassen, sondern hat ebenso andere Risiken in Betracht zu ziehen, wie sie mit der Organisation des Unternehmens und ihren Verfahrensweisen zusammenhängen, solche, die sich auf Personaldaten beziehen oder solche, die mit den bestehenden rechtlichen Beschränkungen zusammenhängen wie etwa dem Datenschutz oder dem Urheberrecht.

Diese multidisziplinäre Wahrnehmung von Risiken ist in der Welt von Informationssicherheitsexperten nicht die Regel. Zu oft wird die Sicherheit von Informationssystemen noch als eine Angelegenheit für Computer- oder Technikexperten betrachtet und darüber hinaus nur begrenzt auf prophylaktische technische Maßnahmen, mit der Folge komplexer Sicherheitssysteme, die in einer Zunahme technischer Kontrollen von zweifelhafter Bedeutung resultieren, die den Datenschutz durchaus beeinträchtigen können.

Selbst wenn der Bedarf an hochausgebildeten Sicherheitsexperten umfassend anerkannt ist, gibt es wenige konkrete strukturierte Initiativen, um die bestehenden Erwartungen zu erfüllen. Oft ist der Begriff eines Informationssicherheitsberaters weder eingeführt, definiert noch durch gesetzliche Regelungen umschrieben. Der Zugang zu diesem Beruf ist einem Zertifizierungsprozess überlassen, der durch private Institutionen organisiert wird.

Empfehlungen

Angesichts dieser Situation empfiehlt die Arbeitsgruppe angesichts der erstrangigen Rolle, die die Sicherheit von Informationssystemen und der Datenschutz beim ordnungsgemäßen Funktionieren von Organisationen spielen, dass:

– das Konzept eines Informationssystemssicherheitsberaters unterstützt wird, der dem CISO-Konzept (Corporate Information Security Officer) entspricht, das in verschiedenen internationalen Normen und Veröffentlichungen beschrieben wird, und das alle notwendigen Datenschutzaspekte umfasst.

– Angesichts der Verantwortlichkeiten, die mit der Ausübung einer solchen Funktion verbunden sind, besteht unzweifelhaft der Bedarf höherer Professionalität. Sehr oft erfordern diese Funktionen einen Hochschulabschluss. Demgemäß sollte eine akademische oder berufsbildende Qualifikation für Informationssystemssicherheitsberater eingeführt werden, die eine Ausbildung gewährleistet, die die nationalen rechtlichen und kulturellen Traditionen berücksichtigt und die so neutral und unabhängig von wirtschaftlichen Interessen ausgestaltet ist wie irgend möglich. Zertifiziert werden sollten mit der Qualifikation alle notwendigen technischen Kenntnisse über Sicherheit, die einschlägigen Managementfähigkeiten, Wissen darüber, wie Sicherheit am besten organisiert werden kann, Kenntnis fundamentaler Datenschutzregelungen und schließlich alle relevanten rechtlichen Kenntnisse, die Sicherheitsberater in die Lage versetzen, ihre Rolle innerhalb der Organisation korrekt auszufüllen.

Working Paper on Cyber Security Curricula Integrating National, Cultural and Jurisdictional (Including Privacy) Imperatives

Information Systems Security

In the early stages of computerization, information systems security was predominantly concerned with modest stand-alone systems in closed networks and was accordingly limited in scope to the adoption of relatively simple rules of physical, computer and logical security.

Subsequently, the proliferation of more and more powerful personal computers, the popularization of new information and communication technologies, the widespread use of the Internet, and the increasing dependence of human activities on the proper functioning of information systems have made the situation more complex.

Today, information systems security can no longer just be limited to palliative countermeasures vis-à-vis technological security threats but needs to involve fundamental changes to behavior patterns by all the participants in order to address the pervasive threats posed by cyber security to human values and human rights.

This new global and systemic approach of the information security has been underlined and put forward by the OECD whose publication *"Guidelines for the security of information systems and networks"* includes a recognition of the need to develop a real 'culture of security'[1].

Information systems security vs. personal data protection

Today, to attain their respective objectives, all the organizations, whether governmental or private, are required to collect, process and retain an increasing volume of data including more personal data within their information systems.

Privacy is a fundamental human right and the valid protection of personal data cannot be achieved without adequate security. This has already been recognized in 1980 by the *"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"*[2]. Whilst security is mandatory to achieve privacy, personal data benefit from specific statutory protection compared with other data and their security requires often a totally different approach. The fundamental data protection principles such as the right of oblivion (right to erasure of obsolete data), the right of access, the limitation of collection and use and the proportionality principle, are regrettably not basic principles to which security professionals necessarily subscribe.

Information Security Professionals

Nowadays information systems security has to deal not just with the technological risks of the various computer platforms, networks, protocol or others components

[1] Recommendation of the OECD Council at its 1037th Session on 25 July 2002: *"OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security"*.

[2] Recommendation by the Council of the OECD adopted on 23rd September, 1980: *"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"* – Security safeguard principles.

of the information systems but has also to take into account other risks such as those connected with the organization of the company, with its work method, those linked to its personnel or those concerned with the legal constraints in force such as data protection or intellectual property.

This multidisciplinary perception of the risks is not the rule in the world of information systems security professionals. Too often, information systems security is still considered just as a computer or technical expert business and then merely limited to prophylactic technical measures, with as a consequence, complex security systems based on a proliferation of technical controls of dubious relevance that may compromise personal privacy.

Even if the need for highly skilled security professionals is more widely recognized, few concrete structural initiatives are taken to meet the existing expectations in this domain. Often the concept of the Information Systems Security Adviser is neither introduced, defined nor framed by any legal text and access to the "profession" is left to a certification process organized by private international companies.

Recommendations

Vis-à-vis this situation, the Working Group, quite aware of the primordial roles that information systems security and data protection play in the proper functioning of any organization, recommends that:

– The concept of Information Systems Security Adviser, corresponding to the CISO concept (Corporate Information Security Officer) described in several international standards[3] and publications[4] and which includes all the necessary data protection aspects, should be supported.

– In view of the responsibilities involved when carrying out such a function there is undoubtedly a need for greater professionalism. Very often such functions require university degrees. Accordingly, an academic or professional qualification should be dedicated to Information Systems Security Advisers that would provide an education according to their national legal and cultural traditions and that would be as neutral and independent as possible of any commercial interests. This qualification should certify all the necessary technical security

[3] ISO 13335: *"Information technology – Security techniques – Management of information and communications technology security"* and ISO 13569: *"Banking and related financial services – Information security guidelines"*.

[4] Different documents published by different national organizations such as NIST *(National Institute of Standards and Technology)* – US, CSE *(Communications Security Establishment)* – Canada and DCSSI *(Direction Centrale de la Sécurité des Systèmes d'Information)* – France.

skills, the relevant management skills, the knowledge of how security can best be managed, knowledge of fundamental data protection concepts and finally all relevant legal skills[5] that would enable security advisers to fulfill their role correctly within an organization.

2005

37. Sitzung, 31. März und 1. April 2005, Madeira, Portugal

Zweites Arbeitspapier zum Datenschutz bei Online-Wahlen in Parlamentswahlen und Wahlen zu anderen staatlichen Gremien

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat bei ihrer 30. Sitzung am 28. August 2001 in Berlin ein Arbeitspapier zum Datenschutz bei Online-Wahlen in Parlamentswahlen und Wahlen zu anderen staatlichen Gremien angenommen[1].

Seitdem sind in mehreren Ländern e-voting-Projekte (Projekte mit elektronischen Abstimmungsverfahren) durchgeführt worden. Diese Projekte haben neue Erkenntnisse und Analysewerkzeuge aufgrund ihrer Auswertung erbracht.

Die Arbeitsgruppe gibt deshalb die folgenden zusätzlichen Empfehlungen:

Elektronische Abstimmungssysteme müssen das Wahlgeheimnis, die Privatsphäre der Wählenden und die Vertraulichkeit des Wahlverfahrens garantieren. Die elektronische Wahl im Wahllokal, ohne dass Daten der Wählenden oder abgegebene Stimmen über eine elektronische Infrastruktur übermittelt werden, müssen die Vertraulicheit, Integrität und Verfügbarkeit des Systems durch folgende Vorkehrungen sicherstellen:

– Die Hard- und Software sollte einer technischen und organisatorischen Vorabkontrolle unterworfen werden, die unter der Aufsicht der zuständigen Wahlbehörde/des zuständigen Wahlamtes (oder einer von dieser/diesem bestimmten unabhängigen Stelle) durchzuführen ist, und

[5] ISO/IEC 17799 “Information technology – Code of practice for information security management” expressly refers to national laws which have to be followed even if the standard is complied with.

[1] S. <http://www.datenschutz-berlin.de/doc/int/iwgdpt/online_voting.htm

– das System (Hard- und Software) sollte der zuständigen Wahlbehörde angezeigt werden; auch sollte die Software mit einer elektronischen Signatur zertifiziert werden, um seine Integrität und Transparenz zu gewährleisten.

Die Übermittlung personenbezogener Daten über die wählenden Personen und die abgegebenen Stimmen über ein Netz, das Online-Wahlbüros verbindet, enthält nicht genügend Sicherheitsgarantien, wenn die Übermittlung nicht in einem virtuellen privaten Netz (Virtual Private Network) stattfindet.

Die Arbeitsgruppe empfiehlt als Grundlage der weiteren Diskussion die Terminologie der Empfehlung R (2004) 11 des Ministerkomitees des Europarates an die Mitgliedstaaten über rechtliche, verfahrensmäßige und technische Standards für elektronische Abstimmungen (e-voting) vom 30. September 2004[2].

Anhang

In dieser Empfehlung werden die folgenden Begriffe mit folgender Bedeutung verwandt:

- Authentifizierung: die Vergewisserung/Überprüfung der behaupteten Identität einer Person oder eines Datensatzes;

- Abstimmung/Wahl: das rechtlich anerkannte Verfahren, in dem ein Wähler oder eine Wählerin seine Wahlentscheidung ausdrücken kann;

- Kandidat: eine zur Wahl stehende Person und/oder Gruppe von Personen und/oder politische Partei;

- Stimmabgabe: Einwurf des Stimmzettels in die Wahlurne;

- e-Wahl oder e-Referendum: eine politische Wahl oder ein Referendum, bei der oder dem elektronische Verfahren in einer oder mehreren Phasen eingesetzt werden;

- Elektronische Wahlurne: das elektronische Verfahren, in dem Stimmen vor der Auszählung gespeichert werden;

- e-voting: eine elektronische Abstimmung oder ein elektronisches Referendum, bei dem zumindest die Stimmabgabe automatisiert erfolgt;

[2] Die Empfehlung ist abrufbar unter <http://www.coe.int/T/e/integrated_projects/democracy/02/_Activities/02_e-voting/>

- Netzbasiertes e-voting: e-voting, bei dem die Stimmabgabe mit einem Gerät erfolgt, das nicht von einem Wahlvorstand kontrolliert wird;
- Versiegelung: der Schutz von Informationen dergestalt, dass sie nicht ohne Zusatzinformationen oder Mitteln genutzt oder interpretiert werden, die nur bestimmten Personen oder Stellen zugänglich sind;
- Stimme: der Ausdruck einer Wahlentscheidung;
- Wähler oder Wählerin: ein Person mit Stimmrecht bei einer bestimmten Wahl oder in einem bestimmten Referendum;
- Abstimmungskanal: die Methode/das Verfahren, in dem der Wähler oder die Wählerin abstimmen kann;
- Wahlmöglichkeiten: die Alternativen, zwischen denen durch die Stimmabgabe bei einer Wahl oder einem Referendum gewählt werden kann;
- Wählerverzeichnis: Liste der wahlberechtigten Personen.

37th meeting, 31st March and 1st April 2005, Madeira, Portugal

Second Working Paper on Data Protection and Online Voting in Parliamentary and other Governmental Elections

The International Working Group on Data Protection in Telecommunications adopted at its 30th meeting on 28 August 2001 in Berlin a Working Paper on data protection and online voting in parliamentary and other governmental elections.[1]

Since then, remote e-vote projects have been carried out in several countries. Those projects have generated new information and more analysis tools, resulting from their evaluation.

The Working Group therefore makes the following additional recommendations:

Electronic voting systems have to guarantee the secrecy of the vote, the privacy of the voter and the confidentiality of the voting procedures. The electronic vote in polling station, without voter's data transmission or votes transmission through an

[1] See <http://www.datenschutz-berlin.de/doc/int/iwgdpt/online_voting.htm>).

electronic infrastructure has to guarantee the confidentiality, integrity and availability of the system by the following procedures:

– the hard- and software should be submitted to a prior technical and organisational audit, carried out under the supervision of the electoral competent public body (or independent body designated by the electoral competent authority) and

– the system (hard- and software) should be notified to the electoral competent public authority and the software should be certificated with a digital signature, in order to guarantee the integrity and transparency of the system.

The transmission of personal data regarding the voters and the votes cast, through a network that connects online polling stations, does not provide enough guarantees, unless the transmission is done in a secure virtual private network.

For further discussion the Working Group recommends to proceed on the basis of the terminology of the Council of Europe Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting adopted on 30 September 2004[2].

Annex

In this Recommendation the following terms are used with the following meanings:

- authentication: the provision of assurance of the claimed identity of a person or data;

- ballot: the legally recognised means by which the voter can express his or her choice of voting option;

- candidate: a voting option consisting of a person and/or a group of persons and/or a political party;

- casting of the vote: entering the vote in the ballot box;

- e-election or e-referendum: a political election or referendum in which electronic means are used in one or more stages;

[2] The Recommendation is available at <http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/>)

- electronic ballot box: the electronic means by which the votes are stored pending being counted;
- e-voting: an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote;
- remote e-voting: e-voting where the casting of the vote is done by a device not controlled by an election official;
- sealing: protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities;
- vote: the expression of the choice of voting option;
- voter: a person who is entitled to cast a vote in a particular election or referendum;
- voting channel: the way by which the voter can cast a vote;
- voting options: the range of possibilities from which a choice can be made through the casting of the vote in an election or referendum;
- voters' register: a list of persons entitled to vote (electors).

38. Sitzung, 6. und 7. September 2005, Berlin

Arbeitspapier zu Web Browser Caching („Zwischenspeicherung") von personenbezogenen Daten bei öffentlichen Internet-Zugängen (z. B. Internet-Cafes)*

1. Einleitung

In Internet-Cafes besteht die Möglichkeit gegen Entgelt oder kostenlos Zugang zum Internet zu erhalten. Als Gratisdienstleistung wird dies mitunter auch in

* Wegen Besonderheiten in der nationalen Gesetzgebung kann das Papier von Italien nicht mitgetragen werden.

öffentlichen Bibliotheken und Schulen angeboten. In diesen von mehreren Personen genutzten Umgebungen kommunizieren die Nutzer mit ihrer Familie oder Freunden, nehmen berufliche oder andere Verpflichtungen wahr und führen online Bankgeschäfte aus. Dies macht Internet-Cafes zu einem Ziel für Kriminelle, die personenbezogene Daten „stehlen". Mit dem steigenden Bewusstsein für die Auswirkungen des „Identitätsdiebstahls" (ID theft), erhält die Rolle der Betreiber von Internet-Cafes bei der Bekämpfung dieses Problems eine immer größere Bedeutung.

2. Probleme

Jüngste Veröffentlichungen über Identitätsdiebstahl und seine Auswirkungen auf die Betroffenen unterstreichen Folgendes:

– Risiken bei der Nutzung des Internet für persönliche Kommunikation

– Datensicherheitsaspekte in Internet-Cafes

– Mangelhafte Betriebsorganisation von Internet-Cafes, die persönlichen Informationen der Nutzer gefährden können.

Die Clientseitige Zwischenspeicherung von Webseiten-Informationen ist seit langem als Sicherheits- und mögliches Datenschutzproblem erkannt. Die Clientseitige Zwischenspeicherung führt zu einer temporären Speicherung der Kopien von Webseiten durch die Webbrowser Software auf der Festplatte des Nutzerrechners. Alle üblicherweise installierten Webbrowser nutzen diese Technik, z. B. ermöglicht sie die Verwendung des „Zurück"-Buttons eines Browsers. Sie sichert auch die Rückkehr zur Quelle einer früher heruntergeladenen Webseite, wenn diese Seite unverändert bleibt.

Ein Sicherheitsproblem tritt auf, wenn personenbezogene Daten Bestandteil einer Webseite sind, die vom Webbrowser zwischengespeichert wird. Die zwischengespeicherte Seite wird, sofern nicht beseitigt, auf dem Computer des Nutzers verbleiben und kann für andere Nutzer mittels des „Zurück"-Buttons, des „History"-Verzeichnisses oder mittels direkter Suche auf der Festplatte des PCs zugänglich sein.

In Internet-Cafes entsteht ein Sicherheitsproblem am Ende der Internet-Sitzung eines Nutzers. Nachfolgende Nutzer sind in der Lage, die Seiten aufzusuchen, die im Zwischenspeicher des Browsers enthalten sind, und auf diese Informationen zu zugreifen. Hier besteht das Risiko, dass angesichts jüngster Veröffentlichungen über Spyware und andere bösartige Programme, die Sicherheitsrisiken, die durch den Browser Cache entstehen, übersehen werden.

3. Empfehlung

Cyber-Cafes sollten sicherstellen, dass alle personenbezogenen Daten, die während einer Internet-Sitzung eines Nutzers gesammelt werden, nach dem Ende der Sitzung (log-out) vollständig entfernt werden. Weiterhin sollte der Nutzer selbst die Möglichkeit haben, den Inhalt des „History"-Ordners zu löschen, bevor ein andern Nutzer Zugang zum System erhält. Es sollte ein Warnhinweis oder -signal (z. B. ein Popup-Fenster) vorgesehen werden, das den Nutzer auf die Löschungsmöglichkeit aufmerksam macht, bevor er sich abmeldet.

38th meeting, 6th and 7th September 2005, Berlin*

Working Paper on Web browser caching of personal information in commercial and public multi-user web access environments (e.g. "Cybercafés")

1. Introduction

A cybercafé provides access to the Internet for a fee or free of charge. A similar free service is sometimes provided at public libraries and schools. In these shared environments, users communicate with family and friends, maintain contact with work and other commitments, and perform Internet banking and other money transfers. This makes cybercafés a target for criminals who steal personal information. With increasing awareness of the impact of ID theft, the role of the cybercafé operator is highlighted in helping to combat this problem.

2. Issues

Recent publicity given to ID theft and its impact on those affected highlights:

– risks associated with using the Internet for personal communication

– security issues in cybercafés

– inadequate housekeeping by cybercafé operators, which can jeopardize the personal information of users.

Client-side caching of information held in web pages has long been recognized as a security and possible privacy issue. Client-side caching involves the temporary storage of copies of web pages by web browsing software on the hard drive of a users' own computer. All commonly installed web browsers use

this technique e.g. it enables the use of a browser's "back button". It also saves return to the source of a previously downloaded web page if the page remains unchanged.

A security problem arises when personal information forms part of a web page cached by a web browser. The cached web page will, unless removed, remain on the user's computer and may be available to other users by means of the browser back-button, history menu, and by direct search of the PC hard drive.

In cybercafés, a security issue arises at the end of a user session. Users who follow may be able to navigate to pages stored in the browser cache and access this information. There is a risk that in the light of publicity given to spyware and other malware, the security hazard presented by the browser cache has been overlooked.

3. Recommendation

Cybercafés should ensure that any personal information collected during a user session is completely removed after the end of that session (log-out). Furthermore the user himself should have the possibility to delete the content of the History folder before any other user is permitted to access the system. There should be a warning message/signal (e.g. a pop-up window) to draw the user's attention to delete the "History" before logging out.

2006

39. Sitzung, 6. und 7. April 2006, Washington D. C., USA

Arbeitspapier zur Online-Verfügbarkeit elektronischer Gesundheitsdaten

Die Arbeitsgruppe hat die steigende Bedeutung Web-basierter Telemedizin bereits in der Vergangenheit unterstrichen[1]. Die Verfügbarkeit elektronischer Gesundheitsdaten in Netzwerken (insbesondere im Internet) während der Lebenszeit

[1] Arbeitspapier zu „netzwerkbasierte Telemedizin", angenommen auf der 31. Sitzung am 26./27. März 2002 in Auckland (Neuseeland) – aktualisiert auf der 38. Sitzung am 6./7. September 2005 (Berlin) <http://ww.datenschutz-berlin.de/attachments/208/wpmed_en.pdf>

eines Patienten und darüber hinaus wirft komplexe zusätzliche Fragen auf. Diese Online-Verfügbarkeit elektronischer Gesundheitsdaten wird hauptsächlich aus den folgenden Gründen favorisiert:

– geringere Kosten für die Verarbeitung medizinischer Daten,

– die unmittelbare, „ubiquitäre“ und (scheinbar) komplette Verfügbarkeit der Daten

  • für Doktoren, um zur Gesundheit des Patienten beizutragen,

  • für die Patienten selbst,

– der Patient könnte seine oder ihre Einwilligung online leichter als offline geben.

Gesundheitsinformationen in Netzwerken könnten auch für Forschungs- und Qualitätsmanagementszwecke genutzt werden. Die Diskussion der weitergehenden Implikationen dieser Entwicklung kann in dieser Arbeitsgruppe nicht geführt werden. Es ist allerdings darauf hinzuweisen, dass elektronische Gesundheitsinformationen in Netzwerken generell das Interesse von Dritten auf sich ziehen werden, wie z. B. von Versicherungsunternehmen und Strafverfolgungsbehörden.

Die besondere Sensitivität von Gesundheitsdaten muss bedacht werden, wenn die Online-Verfügbarkeit elektronischer Gesundheitsdaten erwogen wird. Ärzte haben von je her die Verpflichtung gehabt, Informationen von Patienten unter dem hippokratischen Eid[2] sind vertraulich zu behandeln. Die Aufgabe, sich um die Gesundheit und das Leben des Patienten zu kümmern, war nie eine Rechtfertigung dafür, solche Informationen an Dritte weiterzugeben, die nicht an der Behandlung des einzelnen Patienten beteiligt sind.

Heutzutage ist die Vertraulichkeit medizinischer Informationen in den meisten Ländern durch Strafgesetze geschützt. In einigen Ländern ist sogar die Beschlagnahme medizinischer Daten für Strafverfolgungszwecke verboten, soweit diese Daten im Besitz eines Arztes oder eines Krankenhauses sind. Dieser Standard muss auch aufrecht erhalten werden, wenn elektronische Gesundheitsdaten online gestellt werden sollen. Der Grad des Schutzes für Gesundheitsdaten des Patienten darf nicht davon abhängen, ob diese in konventioneller Weise in einer Akte gespeichert werden oder in einem Netzwerk.

[2] „Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und was man nicht nach außen tragen darf, werde ich schweigen und es geheim halten. Wenn ich diesen Eid erfülle und ihn nicht verletzte, so möge ich mein Leben und meine Kunst genießen, respektiert von allen Menschen für alle Zeiten. Wenn ich ihn aber übertrete oder ihn verletze, dann soll das Gegenteil davon mein Los sein.“

Gesundheitsdaten zählen zu den sensitivsten und privatesten Informationen über den Einzelnen. Die Offenlegung eines Gesundheitszustandes oder einer Diagnose könnte das persönliche und berufliche Leben eines Einzelnen negativ beeinflussen. Sogar die Offenlegung einer geringfügigen Gesundheitsangelegenheit kann für den Patienten peinlich sein und ihn möglicherweise davon abhalten, in Zukunft professionelle medizinische Beratung in Anspruch zu nehmen. Beispiele für Diskriminierung infolge von nicht-authorisierter Weitergabe medizinischer Daten existieren auch bei traditioneller, papierener Aktenhaltung[3]. Betroffenen sind bereits die Einstellung in ein Arbeitsverhältnis, Versicherungen und Kreditzusagen wegen der Offenlegung medizinischer Informationen an unberechtigte Parteien verweigert worden. Die Aufbewahrung medizinischer Daten in elektronischer Form erhöht das Risiko, dass Patienteninformationen unbeabsichtigt offenbart oder in einfacher Weise an unberechtigte Parteien weitergegeben werden können.

Darüber hinaus gibt die Nutzung des unsicheren Internets und – sogar in noch größerem Maße – von ungeschützten drahtlosen Netzwerken[4] zur Speicherung und Übertragung von Gesundheitsdaten Anlass zu besonderen Besorgnissen.

Empfehlungen

Die Arbeitsgruppe gibt daher die folgenden vorläufigen Empfehlungen, die im Lichte zukünftiger rechtlicher Entwicklungen und technologischer Innovationen überprüft werden müssen:

1. Es muss sorgfältig evaluiert werden, welche Kategorien medizinischer Daten in elektronischer Form verfügbar gemacht oder online gestellt werden sollen. Bestimmte Kategorien von Gesundheitsdaten wie genetische oder psychiatrische Daten könnten von der Online-Verarbeitung insgesamt ausgeschlossen werden, oder zumindest besonders strikten Zugriffsbeschränkungen unterliegen müssen.

2. In jedem Fall sollte es der autonomen und freien Entscheidung des Patienten – unterstützt durch nutzerfreundliche Technologien – überlassen werden, welche personenbezogenen Gesundheitsdaten über ihn in einem elektronischen Gesundheitsdatensatz oder in einem Netzwerk gespeichert oder weitergegeben werden sollen, soweit dies nicht ausdrücklich durch nationales Gesetz verlangt

[3] Siehe „Health Privacy Project, Medical Privacy True Stories (10. November 2003), unter http://www.patientprivacyrights.org/site/DocServer/True_Stories.pdf?docID=321.

[4] Vgl. das Arbeitspapier zu potentiellen Risiken drahtloser Netzwerke – allgemeine Empfehlungen; verabschiedet am 15. April 2004 bei 35. Sitzung in Buenos Aires; http://www.datenschutz-berlin.de/attachments/196/1_de.pdf

wird. Diese Entscheidung soll die Möglichkeit der relevanten Gesundheitsdienste oder Ärzte, solche Informationen für Behandlungszwecke zu speichern, unberührt lassen. Die Einwilligung muss immer eine fundamentale Anforderung im medizinischen Bereich sein. Eine strikte Zweckbindung ist auch in einer online-Umgebung essentiell. Zu diesem Zweck müssen Gesundheitseinrichtungen ein internes Zugriffskontrollsystem implementieren, das ausreichend ist, die Privatsphäre des Patienten zu schützen.

3. Die Patienten müssen umfassend über die Art der Daten und die Struktur der elektronischen Gesundheitsdatensätze, in denen die Daten enthalten sind, informiert werden. Die Patienten sollten eine Alternative (konventionelle) Möglichkeit haben, über die auf sie bezogenen medizinischen Informationen Zugriff zu erhalten.

4. Es gibt zusätzliche Herausforderungen für die Vertraulichkeit, die der Online-Verfügbarkeit von Gesundheitsdaten inhärent ist. Die bloße Übertragung von gesetzlichen Standards zur Vertraulichkeit, die in einem traditionellen Umfeld mit papierenen Akten gelten, könnte unzureichend sein, um das Interesse eines Patienten an seiner Privatsphäre zu schützen, wenn elektronische Gesundheitsinformationen online verfügbar gemacht werden. Personenbezogene Gesundheitsinformationen dürfen nur in offenen Netzwerken verarbeitet werden, wenn diese durch starke Verschlüsselung und sichere Authentifizierungsmechanismen geschützt sind. Nur autorisiertem, medizinisch qualifiziertem Personal sollte erlaubt werden, auf spezifische Teile der elektronischen Gesundheitsakte online zuzugreifen, soweit dies unbedingt notwendig ist, und Zugriffe sollten protokolliert werden. Die Daten müssen und richtig und aktuell gehalten werden. Patienten sollte eine nutzerfreundliche Möglichkeit haben, auf seine Protokolldaten online zuzugreifen, um in der Lage zu sein, festzustellen, wer auf seinen oder ihren Gesundheitsdatensatz zugegriffen hat.

5. Die Arbeitsgruppe empfiehlt die Entwicklung von Sicherheitsmindeststandards für den Umgang mit elektronischen Gesundheitsdaten. Diese sollten Standards zur Datenverschlüsselung enthalten, sowie Autorisierungsmechanismen, Transaktionsüberwachungsprozeduren, und Zugriffskontrollsysteme. Die Entwicklung von Grundschutzstandards würde betriebliche Datenschutzbeauftragte und Archivare von Daten in die Lage versetzen, den Patientendatenschutz sicherzustellen und gleichzeitig die Vorteile eines elektronischen Aktenhaltungssystems zu genießen. Die Arbeitsgruppe ermutigt alle Interessengruppen (öffentliche Einrichtungen, den Gesundheitssektor, die Industrie und Standardisierungsorganisationen) datenschutzkonforme Technologien für das elektronische Gesundheitswesen zu entwickeln und anzuwenden, die die notwendige Vertraulichkeit und Sicherheit bieten. Die Arbeitsgruppe begrüßt die gegenwärtig in der Internationalen Organisation für Standardisierung (ISO) diskutierte Initiative zur Verabschiedung eines Sicherheitsstandards für

den Medizin- und Gesundheitssektor (mit dem Entwurf des ISO-Standards 27799, der den Informationssicherheits-Management ISO-Standard 17799 für den Gesundheitssektor adaptiert). Es muss jedoch festgestellt werden, dass diese internationalen Standards nationale Gesetzgebung zum Datenschutz nicht ersetzen können.

Die Arbeitsgruppe lädt den medizinischen Berufsstand und die Öffentlichkeit dazu ein, diese Empfehlungen zu kommentieren.

39th meeting, 6th and 7th April 2006, Washington D.C., USA

Working Paper on Online Availability of Electronic Health Records

The Working Party has highlighted the growing importance of web-based telemedicine earlier[1]. The availability of electronic health records in networks (in particular the Internet) throughout a patient's life and beyond poses complex additional questions. This online availability of electronic health records is favoured mainly on the following grounds:

– lower costs for processing medical data,

– the immediate, "ubiquitous" and (seemingly) complete availability of the data

  • for doctors to benefit the patients' health,

  • for the patients themselves,

– the patient may give his or her required consent online easier than offline.

Health information in networks could also be used for research and quality management purposes. The wider implications of this development are not for this Working Group to be discussed. It should, however, be noted that electronic health information in a network generally might attract the interest of third parties such as insurance companies and law enforcement agencies.

The special sensitivity of health information has to be kept in mind when considering the online availability of electronic health records. Under the Hippocratic

[1] Working Paper on Web-based Telemedicine, adopted on 27 March 2002 at the 31st meeting (Auckland), updated on 6–7 September 2005 at the 38th meeting (Berlin) <http://www.datenschutz-berlin.de/attachments/184/wpmed_en.pdf>

Oath[2] doctors have always had to treat patients' information confidentially. To care for the health and the life of the patient has never been a licence to disclose such information to third parties who are not participating in the treatment of the individual patient.

Today the confidentiality of medical information is protected by criminal law in most countries. In some countries even the seizure of patients' health records for law enforcement purposes is forbidden as long as the records are in the possession of the doctor or a hospital. This standard has to be maintained once electronic health records are to be put online. The level of protection for the patient's health information cannot depend on whether it is stored conventionally in a file or on a network.

Health records are among the most sensitive and private information concerning an individual. Disclosure of a medical condition or diagnosis could negatively impact an individual's personal and professional life. Even the disclosure of a minor health issue could cause embarrassment to a patient, potentially making the individual weary to seek future professional medical advice. Examples of discrimination following the unauthorized release of medical data also exist in traditional paper filing systems[3]. Individuals have been denied employment, insurance, and mortgage approval due to the disclosure of medical information to unauthorized parties. Maintaining health records in an electronic form increases the risk that patients' information could be accidentally exposed or easily distributed to unauthorized parties.

Furthermore, the advent and use of the inherently insecure Internet and even more so of unprotected wireless networks[4] for storing and communicating health information causes particular concern.

Recommendations

Therefore the Working Group makes the following preliminary recommendations which will have to be reviewed in the light of future legal developments and technological innovations:

---

[2] "All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal. If I keep this oath faithfully, may I enjoy my life and practice my art, respected by all men and in all times; but if I swerve from it or violate it, may the reverse be my lot."

[3] See generally, Health Privacy Project, Medical Privacy True Stories (Nov. 10, 2003), available at http://www.patientprivacyrights.org/site/DocServer/True_Stories.pdf?docID=321.

[4] See the Working Paper on potential privacy risks associated with wireless networks – Main Recommendations; adopted on 15 April 2004 at the 35th meeting in Buenos Aires <http://www.datenschutz-berlin.de/attachments/197/1_en.pdf>

1. It must be carefully evaluated which categories of medical data should be made available in electronic form or put online. Certain categories of health information such as genetic or psychiatric data may have to be excluded from online processing altogether or at least be subject to especially strict access controls.

2. In any event it should be left to the patient's autonomous and freely taken decision, supported by means of user-friendly technology, what personal health information is to be stored and disclosed to whom in his or her e-health record or in a network unless expressly required by national law. This decision shall be without prejudice to the possibility for the relevant health care body or doctor to store this information for treatment purposes. Consent must always be a fundamental requirement in the medical scope. Strict purpose limitation is essential also in an online environment. To this end, a health care body needs to implement an internal access control system sufficient to protect the privacy of the patient.

3. The patients shall be fully informed on the nature of the data and the structure of the electronic health record containing them. Patients should have alternative (conventional) means to access medical data related to him or her.

4. There are additional confidentiality challenges inherent to the online availability of health records. Maintaining the legal standard of confidentiality within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online. Personal health information may only be processed in open networks, if it is protected by strong encryption and secure authentication mechanisms. Only authorised, medically qualified personnel should be allowed to access specific parts of the e-health-files online where it is strictly necessary and an audit-trail should be available. The data have to be kept accurate and up-to-date. The patient should have a user-friendly means to access their personal audit trail online to be able to determine who has accessed his or her health record.

5. The Working Group recommends the development of baseline security standards for the handling of electronic health data. The baseline needs to include standards for data encryption, authorization mechanisms, transaction audit procedures, and access control systems. The development of baseline standards would enable information officers and custodians of records to ensure patient privacy protection and enjoy the benefits of an electronic records system. The Working Group encourages all the stakeholders (public authorities, health care sector, industry and standardisation organisations) to develop and apply privacy-compliant e-health technology which provides for the necessary confidentiality and security. The Working Group welcomes the initiatives at present under consideration at the International Organisation for Standardi-

sation (ISO) to approve a security standard for the health and medical sector (with the proposed ISO Standard 27799 adapting the information security management ISO Standard 17799 to the health sector). It has however to be noted that these international standards cannot substitute national legislation on data protection.

The Working Group invites the medical profession and the public to comment on these recommendations.

40. Sitzung, 5. und 6. September 2006, Berlin

Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP)

Das Angebot von Telefondiensten über das Internet (Internet-Telefonie oder „Voice over IP" – VoIP) ist auf dem Vormarsch. Bereits jetzt sind auf DSL oder anderen Breitbandverbindungen basierende Dienste erhältlich, die eine Ersetzung der Festnetztelefonleitungen ermöglichen. Auch haben Anbieter von „traditionellen" Telefondiensten bereits damit begonnen, Dienste unter Nutzung des VoIP-Protokolls anzubieten. Gleichzeitig sind mobile Geräte erhältlich, die es erlauben, Telefonanrufe über das Internet auch in einem mobilen Umfeld abzuwickeln. Diese Entwicklung steht erst noch am Anfang, und weitere Veränderungen in der Telefonlandschaft sind in der näheren Zukunft zu erwarten.

Die Einführung von VoIP-Diensten auf dem Massenmarkt geht einher mit Risiken für die Sicherheit und die Privatsphäre der Benutzer, die in angemessener Weise in einem frühen Stadium angepackt werden müssen.

Die Einführung von VoIP stellt Herausforderungen an die existierenden nationalen und regionalen Regulierungssysteme. Z. B. könnten Anbieter von VoIP-Diensten nicht durch die nationale Gesetzgebung verpflichtet sein, das Telekommunikationsgeheimnis zu wahren, ein Grundrecht, das in vielen nationalen Verfassungen wie auch in internationalen Regulierungsinstrumenten niedergelegt ist.

Viele nationale Regulierungssysteme enthalten gleichfalls Regelungen, die die Verarbeitung von Verkehrsdaten begrenzen, und zwar normalerweise auf Abrechnungszwecke. VoIP-Dienste könnten im Gegensatz dazu mehr personenbezogene Daten verarbeiten, als es für Abrechnungszwecke erforderlich ist (z. B. Daten über ankommende Gespräche), ohne dass der Nutzer sich dessen bewusst ist oder die Möglichkeit hat, solche Verarbeitungen zu begrenzen.

Die Herausforderungen, die die Einführung der Internet-Telefonie für das Telekommunikationsgeheimnis mit sich bringt, dürfen nicht unterschätzt werden[1]: VoIP-Telefone sind technisch gesehen Computer, die mit dem Internet verbunden sind. Als solche sind sie Ziel von Angriffen jeder Art, die alltäglich im Internet stattfinden. Die verschiedenen Protokolle (z. B. das weithin genutzte SIP-Protokoll) implementieren ebenfalls bestimmte datenschutzbezogene Funktionen in verschiedener Weise. So kann z. B. die Unterdrückung der Rufnummer des Angerufenen für Gespräche zwischen VoIP-Telefonen nicht verfügbar seien.

Der Inhalt von Nachrichten in VoIP-Diensten wird über ein Netzwerk von im Vergleich mit dem Festnetz relativ unsicheren Knoten geleitet und damit verwundbar für mögliche Attacken einer potenziell großen Anzahl anderer Nutzer. Es ist daher von großer Bedeutung, sowohl Steuerungsinformationen als auch den Inhalt der übertragenen Nachrichten zu verschlüsseln. Da auch verschlüsselte Nachrichten aufgezeichnet und zu einem späteren Zeitpunkt decodiert werden können, ist eine hinreichend sichere Verschlüsselungsmethode erforderlich.

Die Sicherheit kann auch gefährdet sein, wenn VoIP-Technologien innerhalb eines Unternehmens oder einer Einrichtung der öffentlichen Verwaltung als Ersatz für konventionelle Nebenstellenanlagen eingesetzt wird. Sicherheitsaspekte müssen in Betracht gezogen werden, wenn VoIP-Technologie eingeführt wird.

Das Fernmeldegeheimnis hat seit der Gründung der Arbeitsgruppe im Mittelpunkt ihrer Tätigkeit gestanden[2]. Das Prinzip der Vertraulichkeit von Telefongesprächen wird in den Verfassungsdokumenten vieler Länder garantiert. Bei jeder Verarbeitung personenbezogener Daten müssen angemessene Maßnahmen für die Netzwerke und Server getroffen werden, die zur Erbringung von VoIP-Diensten genutzt werden, um die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der übertragenen Daten zu garantieren[3].

Im Lichte des oben Gesagten gibt die Arbeitsgruppe die folgenden Empfehlungen:

---

[1] Eine im Jahr 2005 vom Deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) in Auftrag gegebene Studie kam zu dem Ergebnis, dass VoIP-Systeme die Sicherheitsrisiken der IP-Welt erben und darüber hinaus die meisten aus der TK-Welt behalten; vgl. http://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf, S. 134.

[2] Vgl. den Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 14. Konferenz, 29. Oktober 1992, Sydney <http://www.datenschutz-berlin.de/attachments/135/fernm_de.htm>

[3] Vgl. den gemeinsamen Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilateraler Abkommen zum Datenschutz – 10 Gebote zum Schutz der Privatheit im Internet, angenommen auf der 28. Sitzung der Arbeitsgruppe am 13./14. September 2000 in Berlin <http://www.datenschutz-berlin.de/attachments/215/tc_de.htm>

Die Regulierer sind aufgefordert, innerhalb des anwendbaren Regulierungsrahmens wie auch bei der Verhandlung zu internationalen Übereinkommen sicherzustellen, dass Anbieter von VoIP-Diensten verpflichtet werden, mindestens den selben Grad von Sicherheit und Schutz der Privatsphäre sicherzustellen, wie Anbieter traditioneller Festnetz- und Mobiltelefondienste[4].

VoIP-Anbieter und Hersteller von diesbezüglicher Hard- und/oder Software sind aufgefordert,

1. ihre Kunden über Risiken für die Sicherheit und die Privatsphäre von VoIP-Diensten[5] und möglichen Abhilfen zu informieren[6],

2. angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzfreundliche Nutzung von VoIP-Diensten zu gewährleisten,

3. interoperable Ende-zu-Ende-Verschlüsselungseinrichtungen als ein Standardmerkmal ihrer Dienste ohne zusätzliche Kosten anzubieten,

4. sicherzustellen, dass Sicherheits- und Datenschutzmerkmale ihrer Produkte standardmäßig aktiviert sind,

5. sich bemühen, zügig jegliche Sicherheits- oder Datenschutzlücken aus den Protokollen und der genutzten Hard- und/oder Software zu eliminieren[7],

6. Offene Standards zu nutzen und ihre Nutzer und die breite Öffentlichkeit über die genutzten Protokolle und/oder Produkte zu informieren,

7. den Umfang der standardmäßig gespeicherten und verarbeiteten personenbezogenen Daten (z. B. Verkehrsdaten) auf das Maß zu begrenzen, das für die Erbringung und Abrechnung (soweit erforderlich) eines Dienstes nötig

[4] VoIP-Datenschutzstandards sollten nicht an ein Mindestmaß von Datenschutzerwartungen in der Telefonie gebunden sein. Obwohl Einrichtungen zum Datenschutz in traditionellen Telefondiensten als unvollständige Beispiele wünschbarer Einrichtungen dienen können, sollten VoIP-Systeme unter der Maßgabe entwickelt werden, welche Einrichtungen am besten die Privatsphäre schützen können, egal ob diese in traditionellen Telefonnetzen implementiert worden sind oder nicht.

[5] Unter anderem sollten VoIP-Anbieter ihre Nutzer informieren, wenn deren persönliche Informationen verloren gegangen sind, gestohlen wurden oder auf sie durch unauthorisierte Parteien zugriffen worden ist, während sie im Besitz des Diensteanbieters waren.

[6] Im Fall des Angebots von VoIP über WLAN-Dienste sollte dies Information über Risiken und deren Beseitigung für WLAN-Technologie einschließen, vgl. das Arbeitspapier zu potentiellen Risiken drahtloser Netzwerke – allgemeine Empfehlungen (14. – 15. April 2004, Buenos Aires);
<http://www.datenschutz-berlin.de/attachments/196/1_de.pdf>

[7] Dies könnte eine Erweiterung oder Veränderung der genutzten Protokolle (z. B. des SIP-Protokolls) um eine Kontrolle des Nutzers über die übertragene Protokollinformation und deren Anzeige auf Einrichtungen des Angerufenen und des Anrufers einschließen.

ist, falls nicht zusätzliche Speicherungen und Verarbeitungen von Daten ausdrücklich gesetzlich vorgeschrieben sind,

8. datenschutzrelevante Merkmale wenigstens in der selben Art wie im Festnetz anzubieten (z. B. die Unterdrückung der Anzeige der Rufnummer des Anrufers beim Angerufenen)[8],

9. keine Daten über die Erreichbarkeit eines Nutzers oder seinen physischen Aufenthaltsorts zu speichern, außer zur Erbringung von Notrufdiensten oder, soweit die Daten in anonymer Form gespeichert werden, zur Verbesserung der Servicequalität. Solche Informationen sollten nicht länger gespeichert werden, als es für diese Zwecke erforderlich ist, und sie sollten auch nur für diese Zwecke zugänglich sein. Diese Information sollte anderen Kunden – einschließlich anderen Teilnehmern irgendeines Kommunikationsvorganges – nicht angezeigt werden, soweit nicht der Betroffene willentlich und ausdrücklich eine entsprechende Wahl getroffen hat. Ein Nutzer sollte in der Lage sein, auszuwählen, welche anderen Nutzer (wenn überhaupt) seine Verfügbarkeits- und Aufenthaltsinformationen sehen können. Verfügbarkeits- und Aufenthaltsinformationen sollten nicht verkauft oder für gezielte Werbung genutzt werden, soweit der Nutzer darin nicht ausdrücklich eingewilligt hat.

10. die Möglichkeit aufrecht erhalten, Telekommunikationsnetze durch öffentliche Zugangspunkte in anonymer Weise zu nutzen.

40th meeting, 5th and 6th September 2006, Berlin

Working Paper on Privacy and Security in Internet Telephony (VoIP)

The provision of telephone services over the Internet (internet telephony or "voice over IP" – VoIP) is on the increase. Already now services based on DSL or other broadband connectivity are available that allow for a complete replacement of fixed telephone lines. Providers of "traditional" telephone services have also begun to deliver services using the VoIP protocol. At the same time mobile equipment becomes available allowing for placing phone calls over the Internet also in a mobile environment. This development is only at its beginning, and further changes of the telephony landscape are likely to occur in the near future.

[8] Vgl. oben Fußnote 4 oben

The introduction of VoIP services to the mass market comes with risks for security and privacy of its users that need to be tackled appropriately at an early stage.

The introduction of VoIP poses challenges to the existing national and regional regulatory regimes. For example, providers of VoIP services may not be obliged by national laws to provide for telecommunications secrecy, which is a basic right laid down in many national constitutions as well as in supranational regulatory instruments.

Many national regulatory regimes also contain provisions restricting the processing of traffic data, normally bound to billing needs. VoIP services may instead process more personal data than necessary for billing purposes (e.g. call records for incoming calls) without user being aware of or being able to restrict such processing.

The challenges the introduction of internet telephony will pose for the secrecy of telecommunications should not be underestimated[1]: VoIP telephones are technically speaking computers connected to the Internet. As such they are targets for attacks of any kind common on the Internet today. The different protocols (e.g. the widely used SIP protocol) also implement certain privacy-related functions in different ways. For example, calling line identification restriction may not be available for calls between VoIP telephones.

The content of messages in VoIP services is routed over a network of – in comparison with the fixed telephone network – relatively insecure nodes, making them vulnerable to potential attacks by a potentially large number of other users. It is therefore essential to encrypt signalling messages as well as the content of the communication. As encrypted messages may also be recorded and then be decoded at a later stage, a sufficiently secure encryption method is required.

Security may also be at risk when VoIP technology is applied within a company or a body of the public administration as a replacement for conventional PABX systems. Security aspects must be considered when VoIP technology is introduced.

Telecommunications secrecy has been in the focus of the Working Group since it was founded[2]. The principle of inviolability of telephone conversations is

[1] A study commissioned in 2005 by the German Federal Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik – BSI) concluded that VoIP systems inherit the security risks from the IP world, while keeping most of those from the telco world;
cf. http://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf on page 134 (German only).

[2] Cf. e.g. the report of the Working Group on Telecommunication and Media on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the International Conference of Data Protection and Privacy Commissioners 14th Conference, 29. October 1992, Sydney
<http://www.datenschutz-berlin.de/attachments/134/fernm_en.htm>

guaranteed in the constitutional documents of many countries. As with any processing of personal data, appropriate measures must be taken on the networks and servers used for delivering VoIP services to guarantee for availability, confidentiality, integrity and authenticity of the data transmitted[3].

In the light of the above, the Working Group makes the following recommendations:

Regulators are called upon to ensure in the applicable regulatory frameworks as well as when negotiating international agreements that VoIP service providers are obliged to ensure the same level of security and privacy as providers of traditional fixed and mobile telephone services as a minimum[4].

VoIP providers and manufacturers of respective hard- and/or software are called upon to

1. inform their customers about privacy and security risks of VoIP services[5] and possible remedies[6],

2. take appropriate technical and organisational measures to provide for a secure and privacy-friendly use of VoIP services,

3. offer interoperable end-to-end encryption facilities as a standard feature of their service at no additional costs,

4. make sure that security and privacy features of their products are activated by default,

5. strive to swiftly eliminate any security or privacy flaws of the protocols and the hard- and/or software in use[7],

---

[3] Cf. Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements – Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000) <http://www.datenschutz-berlin.de/attachments/216/tc_en.htm>

[4] VoIP privacy standards should not be tied to a baseline of telephone privacy expectations. Although privacy features in traditional telephone services can serve as an imperfect example of desirable features, VoIP systems should be developed with consideration of what features would best protect privacy, regardless of whether they have been implemented in the traditional phone network.

[5] Inter alia, a VoIP provider should notify any user whose personal information has been lost, stolen, or accessed by an unauthorized party while in that service provider's possession.

[6] In the case of VoIP over WLAN services this should include information on risks and remedies for WLAN technology, cf. Working Paper on potential privacy risks associated with wireless networks. Main Recommendations (14–15 April 2004, Buenos Aires); <http://www.datenschutz-berlin.de/attachments/197/1_en.pdf>

[7] This may include extensions or changes of the protocols in use (e.g. the SIP protocol) to allow for user control over the protocol information transmitted and/or displayed on the equipment of the called and the calling party.

6. use open standards and inform their customers and the general public about the protocols and/or products in use,

7. restrict the amount of personal data stored and processed by default (e.g. traffic data) to what is necessary for the provision and billing (as applicable) of the service, unless additional storing and/processing of data is explicitly mandated by law.

8. offer privacy-relevant features at least in the same manner as in the fixed telephone network (e.g. suppression of the presentation of the calling number at the called party)[8],

9. not to collect a user's availability and physical location information except to provide emergency services or, if collected in an anonymous form, to improve service quality. Such information should be stored no longer than those purposes require, and it should be accessible only for those purposes. This information should not be displayed to other customers, including any other party or parties to any communication, unless the data subject affirmatively and explicitly chooses to do so. A user should be able to choose which other users (if any) can see her availability and location information. Availability and physical location information should not be sold or used for targeted advertising without the user's explicit consent.

10. maintain the possibility to use telecommunications networks via public access points in an anonymous way.

Arbeitspapier

Trusted Computing, damit zusammenhängende Technologien zur digitalen Rechteverwaltung, und die Privatsphäre: Einige Fragestellungen für Regierungen und Softwareentwickler

Trusted Computing und die damit zusammenhängenden Technologien zur digitalen Rechteverwaltung (TC/DRM) können für die Privatsphäre viele Vorteile bringen. Verbesserte Sicherheit von Systemen, in denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, ist ein lobenswertes Ziel. Jedoch ist eine informierte und verantwortungsvolle Implementierung dieser komplexen

[8] Cf. footnote 4 above

Technologien notwendig, um unabsichtliche Risiken für die Privatsphäre zu vermeiden[1].

Den Mittelpunkt der Datenschutzrisiken bildet die Einrichtung zur „Fernattestierung" („remote attestation"), einschließlich des Potenzials für einen langfristigen Mangel an Kontrolle über die Dokumente einer Organisation. So besteht z. B. eine der identifizierten Probleme in der Beeinträchtigung des Rechts eines Individuums, über seine bei einer Behörde gespeicherten personenbezogenen Daten Auskunft zu erhalten, wenn die Zugriffsrechte auf das Dokument, das diese personenbezogenen Informationen enthält, abgelaufen sind.

Spezielle Bedingungen können für Regierungen bei der Implementierung von TC/DRM-Technologien wegen ihrer gesetzlichen Verpflichtungen bestehen, die eine Archivierung vorsehen. Aus diesem Grund sind die folgenden Empfehlungen überwiegend, aber nicht ausschließlich an öffentliche Stellen gerichtet. Organisationen des Privatsektors werden in den meisten Fällen ähnliche, möglicherweise sogar gesetzlich festgelegte Verantwortlichkeiten haben.

Empfehlungen

Die Arbeitsgruppe empfiehlt, dass Regierungen die potenziellen Gefährdungen für den Datenschutz und die Langzeit-Aufbewahrung von Daten öffentlicher Stellen erwägen, die aus der unbedachten Implementierung solcher Technologien resultieren könnten. Eine Zusammenarbeit mit anderen Regierungen bei Verhandlungen mit Verkäufern (z. B. Ausschreibungen) könnte der effektivste Weg sein, diesen potenziellen Gefahren zu begegnen.

Regierungen sollten Regelungen etablieren, um sicherzustellen, dass die Vorteile der „von TC/DRM-Technologien in Bezug auf Daten der Regierung nicht von unbeabsichtigten, die Privatsphäre beeinträchtigenden Effekten überwogen werden.

Regierungen sollten die Übernahmen oder Anpassung der von Neuseeland [2]entwickelten Prinzipien und Regelungen erwägen, die nachfolgend zusammengefasst sind:

Regierungen sollten TC/DRM-Technologien nicht in einer Weise implementieren, die

[1] Vgl. den gemeinsamen Standpunkt der Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation „Datenschutz und Urheberrechts-Management", angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000; <http://www.datenschutz-berlin.de/attachments/233/co_de.pdf>

[2] New Zealand State Services Commission: Trusted Computing and Digital Rights Management Principles and Policies, Version 1.0, 25. September 2006.

1. das Recht des Einzelnen auf Auskunft gefährden könnte, oder

2. die Vertraulichkeit und Integrität von Datenbeständen der öffentlichen Verwaltung gefährden könnte, oder

3. den Schutz personenbezogener Informationen gefährden könnte, oder

4. die Sicherheit von Informationssystemen der öffentlichen Verwaltung gefährden könnte.

Die Arbeitsgruppe empfiehlt Software-Entwicklern und Verkäufern von TC/DRM-Produkten und ermutigt sie dazu, sich der Herausforderung, der sich Regierungen bei der Einführung und Implementierung von „Trusted Computing“ und digitaler Rechteverwaltung gegenüber sehen könnten, bewusst zu werden. Einige dieser Probleme mögen von denen der geschäftlichen Nutzer von TC/DRM abweichen, viele von gleicher Natur sein werden. Anbieter sollten sicherstellen, dass sie in der Lage sind, Anforderungen der Regierung im Hinblick auf die Transparenz der Anwendung dieser Systeme und Anwendungen zu entsprechen.

Anbieter könnten häufig vorfinden, dass Regierungen volle Kenntnis und Zustimmung brauchen werden zu:

1. externen Behinderungen im Hinblick auf Datensätze,

2. Datenflüssen, insbesondere solchen, die mit der Erhebung personenbezogener Daten einhergehen,

3. Übermittlungen außerhalb von Regierungssystemen (einschließlich Attestierung und anderen Hintergrundübermittlungen),

4. Regelungen, die den Zugriff auf Informationen öffentlicher Stellen kontrollieren und erlauben, und

5. Datensicherheitsrisiken im Zusammenhang mit schädlichen Inhalten wie z. B. Viren und jeglichen anderen Einflüsse auf die Datensicherheit.

Anbieter sollten darauf vorbereitet sein, Regierungen unabhängige Bestätigungen darüber vorzulegen, dass ihre Systeme in der Weise funktionieren, wie es in der Spezifikation beschrieben ist.

Working Paper

Trusted Computing, Associated Digital Rights Management Technologies, and Privacy: Some issues for governments and software developers

Trusted computing and associated digital rights management technologies (TC/DRM) can bring many benefits for privacy. Improved security of the systems within which personal information is collected, accessed, used, and disclosed is a laudable goal. However, informed responsible implementation of these complex technologies is required in order to avoid unintended risks to personal privacy.[1]

Privacy risks centre on the remote attestation feature but include the potential for long-term lack of control over an organisation's documents. For example, one concern that has been identified is the possible compromise of an individual's right to access personal information held by an agency if the rights to a document containing that personal information have expired.

There can be special issues for governments implementing TC/DRM technologies because of their responsibilities under legislation mandating archiving requirements. For this reason, the recommendations that follow are largely but not exclusively targeted to government agencies. Private sector organisations will in most cases have similar, if not legislated, responsibilities.

Recommendations

The Working Group recommends that governments consider the potential hazards to privacy and the long-term maintenance of official government records that may result from ill-considered implementation of these technologies. Collaboration with other governments in engaging with the vendor community may be the most effective way of responding to those potential hazards.

Governments should establish policies to ensure that the benefits of implementing TC/DRM technologies in relation to government records are not outweighed by unintended privacy-invasive effects.

Governments should consider adoption or adaptation of the principles and policies developed by New Zealand[2] and summarised here as:

---

[1] See also IWGDPT, *Common Position on Privacy and Digital Rights Management*, adopted 4/5 May 2000 < http://www.datenschutz-berlin.de/attachments/234/co_en.pdf>

[2] New Zealand State Services Commission, *Trusted Computing and Digital Rights Management Principles and Policies*, version 1.0, 25 September 2006.

Governments should not implement TC/DRM technologies in ways that may

1. compromise subject access rights, or

2. endanger the confidentiality and integrity of official records, or

3. endanger the privacy of personal information, or

4. compromise the security of government information systems.

The Working Group recommends and encourages software developers and suppliers of TC/DRM products to make themselves aware of the challenges that governments may face in the adoption and implementation of trusted computing and digital rights management technologies. Some of these issues may differ from those faced by business users of TC/DRM, while many will be the same. Suppliers should ensure that they are able to accommodate government requirements for transparency of operation of these systems and applications.

Suppliers may often find that governments will need full knowledge of and consent to:

1. external encumbrances on records,

2. data flows, especially those involving the collection of personal information,

3. communications outside government systems (including attestation and other background communications),

4. regimes that control and permit access to government-held information, and

5. data safety concerns around harmful content such as viruses and any other security implications.

Suppliers should be prepared to provide governments with independent verification that their systems operate as their communications specifications describe.

2007

41. Sitzung, 12. und13. April 2007, St. Peter Port, Guernsey

Arbeitspapier zum grenzüberschreitenden Telemarketing

Hintergrund

Gestützt auf frühere Arbeiten dieser Arbeitsgruppe haben zahlreiche Länder nunmehr legislative Maßnahmen ergriffen, die das Recht des Einzelnen respektieren, den Empfang unverlangter Telemarketing-Anrufe zu verhindern. Zu diesen Maßnahmen zählen die Telekommunikations-Richtlinien der Europäischen Union von 1997 und 2002, die in der Schaffung von Sperr-Registern in einigen Mitgliedstaaten der Europäischen Union mündeten, und in der Einrichtung der US-amerikanischen Sperrliste durch die Federal Trade Commission, während in anderen Rechtsordnungen auf der Einwilligung basierende Regelungen oder Mischungen aus Einwilligungs- und Widerspruchslösungen geschaffen wurden.

Diese Register und die damit verbundenen Durchsetzungsbefugnisse nationaler Behörden haben sich im Großen und Ganzen als recht effektiv zur Verhinderung des Empfangs unverlangter Telemarketing Nachrichten erwiesen, die aus dem selben Land oder Territorium herrühren, in dem sich der Angerufene befindet, waren jedoch weitgehend unwirksam hinsichtlich der Verhinderung von Anrufen aus dem Ausland.

Durch die fallenden Kosten internationaler Telefonanrufe und besonderes die Nutzung des Voice over Internet Protocol ist zu erwarten, dass die Häufigkeit grenzüberschreitender Telemarketing-Anrufe zunehmen wird.

Diese Situation wird verschärft durch die Tatsache, dass viele Werbeanrufe, insbesondere solche aus dem Ausland, häufig keinerlei Informationen über die Rufnummer des Anrufenden enthalten, die ihre Identifikation durch den Anrufer erlauben würden. Darüber hinaus scheint es, dass die Information zur Rufnummernanzeige nicht immer zwischen nationalen und internationalen Netzwerken übertragen wird.

Es scheint gegenwärtig keine Mechanismen zur Zusammenarbeit der Betreiber von nationalen Sperr-Registern zu geben, die eine datenschutzfreundliche Nutzung ihrer Datenbanken durch international operierende Telemarketing-Unternehmen ermöglichen würden.

Jedenfalls wird es sich ohne die Schaffung bindender internationaler Instrumente als sehr schwierig erweisen, das Recht durchzusetzen, keine unverlangten Werbeanrufe aus dem Ausland zu erhalten. Daher müssen alternative technische und organisatorische Maßnahmen erwogen werden.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

- Telemarketing-Unternehmen sollten sich über die anwendbaren Regelungen (Einwilligung und/oder Widerspruch) in den Ländern, in denen sie tätig sind, informieren und diese Regelungen respektieren.

- Telemarketing-Unternehmen sollten verpflichtet werden, ihre Rufnummern bei allen Werbeanrufen zu übertragen, so dass der Angerufene den Anrufer identifizieren und die Löschung von der Anrufliste des Werbetreibenden fordern kann, soweit dies vorgesehen ist, oder sich – zum Beispiel in Rechtsordnungen, die eine Einwilligung vorsehen – bei den zuständigen Behörden beschweren kann.

- Anbieter von Telekommunikationsdienstleistungen sollten zusammenarbeiten, um die Übermittlung der Rufnummer des Anrufenden im Bezug auf Werbeanrufe zwischen nationalen, internationalen und Voice over IP-Netzwerken zu gewährleisten.

- Anbieter von Telekommunikationsdienstleistungen sollten ihren Nutzern ein Verfahren anbieten, in dem diese sich über unverlangte Werbeanrufe beschweren können, und sicher stellen, dass solche Beschwerden an die zuständigen Behörden in dem Land weitergeleitet werden, aus dem der Anruf herrührt.

- Anbieter von Telekommunikationsdienstleistungen sollten den Nutzern eine einfache technische Möglichkeit eröffnen, die Zurückweisung eines ankommenden Werbeanrufs zu signalisieren und, soweit der Angerufene dies wünscht, sollte dieses Signal an den Anrufer übertragen und als Hinweis genutzt werden, dass weitere Anrufe bei diesem Nutzer zu unterbleiben haben.

Die Internationale Arbeitsgruppe ruft die Datenschutzbehörden weltweit auf, ihre Anstrengungen zur Zusammenarbeit untereinander und mit Aufsichtsbehörden im Bereich der Telekommunikation zu intensivieren, um die Aktivitäten von Organisationen, die über Landesgrenzen hinweg unverlangte Werbeanrufe durchführen, zu begrenzen.

41st meeting, 12th and 13th April 2007, St. Peter Port, Guernsey

Working Paper on Cross-Border Telemarketing

Background

Based on the early work of this Working Group, many territories have now implemented legislative measures that respect the right of individuals to prevent the receipt of unsolicited telemarketing calls.

These measures have included the 1991 and 2002 Telecommunications Directives of the European Union, which resulted in the setting up of do-not-call registries in some EU Member States and in the establishment by the US Federal Trade Commission of the US Do-not-call-registry, while other jurisdictions have implemented opt-in regimes or mixes of opt-in and opt-out.

These registries and the associated enforcement powers vested in domestic authorities have, in general, proved quite effective in preventing the receipt of unwanted telemarketing calls that originate from within the subscribers own country or territory, but have been largely ineffective in preventing calls that originate from elsewhere.

With the falling cost of international telephone calls and in particular the exploitation of Voice over Internet Protocol, it is anticipated that the prevalence of cross-border telemarketing calls is likely to increase.

The situation is aggravated by the fact that many telemarketing calls, especially those from abroad tend not to include any Caller Identity information that would permit their identification by the called party. Furthermore, it would appear that Caller Identity information is not always transmitted between domestic and international networks.

There do not appear to be mechanisms at present whereby the operators of all national do-not call registries are able to collaborate in order to facilitate the use of their databases by international telemarketers in a privacy-friendly manner.

In any case, without the creation of binding international instruments, it may prove very difficult to enforce the right not to receive unwanted telemarketing calls from abroad; accordingly, alternative technical and administrative measures need to be devised.

Recommendations

The Working Group recommends that:

- telemarketing companies should inform themselves about the applicable regime (opt-in and/or opt-out) in the countries in which they are operating and respect the respective regulations.

- telemarketing companies should be required to include Caller Identity information in all marketing calls such that a called subscriber is able to identify the caller and to request removal from the marketers call list as applicable, or to file complaints with the relevant authorities e.g. in jurisdictions where opt-in is required;

- telecommunications service providers should cooperate to ensure the transmission of Caller Identity information relating to marketing calls between domestic networks, international networks and voice over IP networks;

- telecommunications service providers should provide a mechanism for subscribers to complain about unsolicited telemarketing calls and ensure that such complaints are forwarded to the appropriate authorities in the country in which the calls appear to originate;

- telecommunications service providers should enable telephone subscribers to have a simple technical means to signal a rejection of an incoming telemarketing call and, if the called person so wishes such a rejection should be transmitted to the caller and used as an indicator that further calls to that subscriber are to be suppressed;

The International Working Group calls upon Data Protection and privacy authorities worldwide to intensify their efforts to co-operate with each other and with telecommunications regulators in order to limit the activities of unsolicited telemarketing organisations operating across country borders.

42. Sitzung, 4. und 5. September 2007, Berlin

Arbeitspapier E-Ticketing in öffentlichen Verkehrsmitteln

1. Die technologische Entwicklung im Bereich der Chipkarten und das Streben nach erhöhter Effizienz und Kosteneffektivität beim Management von Dienstleistungen im öffentlichen Verkehr –dies betrifft integrierte Eisenbahnen, U-Bahn und Flächentransportdienstleistungen – haben zu einer wachsenden Nutzung innovativer E-Ticketing Systeme geführt.

   Solche Systeme arbeiten mit elektronischen Karten, die gewöhnlich personalisiert sind und die vornehmlich für Transportdienstleistungen, aber zunehmend auch zur Bezahlung damit zusammenhängender anderer Leistungen genutzt werden können (z. B. für elektronische Bezahlung von Parkgebühren bei Pendlern)[*].

2. Die Chipkarten enthalten einen Mikroprozessor, der Informationen einschließlich personenbezogener Daten speichert (dazu können z. B. die Chipidentifizierungsnummer, die Nummer des Abonnnements des Benutzers sowie die Zeit, das Datum und die Nummer des Gerätes zur Entwertung oder zur Überprüfung der Gültigkeit der Fahrkarten gehören); in manchen Fällen arbeiten sie mit RFID/Near Field Communication (NFC)Technologie.

   Die Nutzung solcher Chipkarten beinhaltet daher die Verarbeitung von verschiedenen unmittelbar und/oder mittelbar zuordenbaren personenbezogenen Informationen:

   - Zu dem Zeitpunkt, zu dem die Karten an die Benutzer ausgegeben werden;
   - Jedes Mal, wenn die Karten benutzt werden, dank der Identifikationsnummern, die jedem Abonnenten zugeordnet sind und die durch Geräte zur Entwertung oder zur Überprüfung der Gültigkeit der Fahrkarten gesammelt und dann möglicherweise in Echtzeit in den Datenbanken der Transportunternehmen gespeichert werden.

   In diesem Kontext müssen besonders die so genannten Validierungsdaten (Daten über die Entwertung oder Überprüfung der Gültigkeit) beachtet werden, deren Verarbeitung – insbesondere die Speicherung von Zeit und Ort der Entwertung oder Überprüfung – es ermöglicht, die Bewegungen und Aufenthaltsorte einzelner Benutzer zu verfolgen.

[*] Andere Zahlungsformen sind z. B. Barzahlung, Zahlung über Mobiltelefon, etc.

3. Die Informationen, die öffentliche Transportunternehmen im Rahmen der Erbringung ihrer Dienstleistungen verarbeiteten, einschließlich der Informationen, die zum Zeitpunkt der Entwertung oder Überprüfung der Karte gespeichert werden, können für verschiede Zwecke genutzt werden, wie z. B.:
   - die Bereitstellung von Transportdienstleistungen,
   - die Bekämpfung von Betrug beim E-Ticketing (wenn Chipkarten verloren, gestohlen oder ohne Autorisierung kopiert werden),
   - Werbung,
   - die Aufteilung der Einnahmen unter verschiedenen Beteiligten, wenn öffentliche Transportdienstleistungen gemeinsam durch mehrere Transportunternehmen erbracht werden,
   - die Analyse aggregierter Daten über Verkehrsflüsse, um die Effizienz der erbrachten Dienstleistungen zu steigern.

Empfehlungen

Die Arbeitsgruppe empfiehlt:

Vorabkontrolle (Privacy Impact Assessment)
Das Recht der Kunden auf den Schutz ihrer personenbezogener Daten muss bereits beim Entwurf und im Rahmen der Entwicklung von Informationssystemen der Transportunternehmen berücksichtigt werden; grundsätzlich sollten das Recht auf persönliche Freizügigkeit und die Anforderungen effizienten öffentlichen Verkehrs miteinander in Einklang gebracht werden.

Anonymität
Verkehrsbetriebe und Transportunternehmen sollten ihren Kunden alternativ Möglichkeiten zur anonymen Nutzung (ohne unbillige Hindernisse) anbieten, z. B. Barzahlung oder anonyme E-Tickets.

Wo Anonymität aus technischen Gründen nicht angeboten werden kann, müssen die folgenden Empfehlungen beachtet werden:

Datenschutzinformation und Transparenz
Verkehrs- oder Transportunternehmen, die E-Ticketing-Systeme nutzen, sollten die Betroffenen unmissverständlich über die Verarbeitung ihrer personenbezogenen Daten informieren. Die Betroffenen sollten in der Lage sein, die spezifischen Zwecke leicht zu verstehen, die von den Unternehmen verfolgt werden, welche Arten von personenbezogenen Daten über sie gesammelt und gespeichert werden, und wie diese Informationen genutzt werden.

Datensparsamkeit und Speicherungsdauer
Insbesondere in Bezug auf die Verarbeitung der Reisedaten der Nutzer sollten die Informationssysteme von Transportunternehmen so geplant und entwickelt werden, dass sie die Nutzung anonymer Daten priorisieren. Wenn (direkt oder indirekt) personenbezogene Daten genutzt werden, sollten diese Informationen für die kürzestmögliche Zeitdauer gespeichert (und danach gelöscht) und die gesetzliche Zweckbestimmung der Verarbeitung beachtet werden – grundsätzlich sollten die betreffenden Informationen nicht länger als ein paar Tage nach ihrer Erhebung gespeichert bleiben.

Sicherheit
Die Sicherheitsmaßnahmen beim Zugriff auf personenbezogene Daten sollten ein Überwachungssystem zur Verhinderung des Missbrauchs von Informationen umfassen. Verkehrsunternehmen sollten sicherstellen, dass der Schutz der Privatsphäre registrierter Nutzer garantiert wird, wenn sie ihren Partnern und ihren eigenen Mitarbeitern den Zugriff auf ihre Datenbanken eröffnen.

Werbung
Ein Verkehrs- oder Transportunternehmen sollte die freiwillige und informierte, vorherige Einwilligung seiner Kunden für die Nutzung personenbezogener Daten für eigene Werbezwecke oder die Nutzung durch verbundene Partnerunternehmen für unverlangte Werbung gegenüber dem Reisenden einholen. Diese Einwilligung sollte sich von der Zustimmung zu allgemeinen Geschäftsbedingungen unterscheiden.

Zahlungsnachweis
Soweit z. B. zur Kostenerstattung oder aus steuerlichen Gründen ein Zahlungsnachweis über einzelne Reisen erforderlich ist, sollten dafür datenschutzfreundliche Lösungen angeboten werden.

Verhaltensregeln
Die Entwicklung von Verhaltensregeln zum Datenschutz sollte gefördert werden. Insbesondere im Hinblick auf die Verarbeitung von Bewegungsdaten der Nutzer sollten Informationssysteme von Transportunternehmen unter Priorisierung der Nutzung von anonymen Daten geplant und entwickelt werden.

Systemdesign
Die Systementwicklung sollte so erfolgen, dass personenbezogene Daten von Reisedaten getrennt werden (2-Komponenten-Modell). Eine zentrale Speicherung sollte auf aggregierte und/oder anonyme Transaktionen beschränkt werden. Karteninhaber sollten Daten über die Nutzung ihrer Karten kontrollieren können.

42nd meeting, 4th and 5th September 2007, Berlin

Working Paper E-Ticketing in Public Transport

1. Technological evolution in smart cards and the search for increased efficiency and cost-effectiveness in managing public transport services – as provided via integrated railway, subway and surface transport services – have resulted in the growing use of innovative e-ticketing systems.

   Such systems work by means of electronic cards, usually personalised, that are predominantly used for transport services but may increasingly be used to purchase related services (e.g. to pay commuter parking fees).*

2. Smart cards contain a chip to store information, including personal information (which may include a chip identifier, the number of the user's subscription contract as well as time, date and code number of the card validation device); in some cases they operate via RFID/Near Field Communication (NFC) technology.

   The use of such cards therefore entails the processing of several items of directly and/or indirectly identifiable personal information:

   - at the time the cards are issued to users;
   - each time the cards are used, thanks to the identifiers that are associated with every subscriber and collected by the validation devices to be subsequently stored (possibly in real time) in the databases of transport companies.

   Special attention should be paid in this context to the information related to the so-called validation data, whose processing – in particular the storage of the time and place of validation – allows tracking the individual users' movements and whereabouts.

3. The information processed by public transport companies in providing their services, including the information that is stored at the time a card is validated, may be processed for diverse purposes – such as, in particular,

- to provide the transportation service;
- to fight fraud in e-ticketing (if a smart card is lost, stolen or duplicated without authorisation);
- to carry out marketing activities;

* Other ways to pay may include, cash, mobile phones, etc.

- to allocate revenues among several entities, if the public transportation services are provided jointly by several transportation companies;
- to analyse aggregate data on traffic flows in order to enhance effectiveness of the services provided.

Recommendations

The Working Group recommends that:

Privacy Impact Assessment
The information systems of transport companies should be designed and implemented by taking into account the customers' right to protection of their personal data; generally speaking, they should reconcile the right to free movement of individuals with the requirements of effective public transportation.

Anonymity
The Public Transport Authority (PTA) or transport company should provide alternative ways for customers to travel anonymously (without undue obstacles), e.g. cash or an anonymous e-ticket.

Where anonymity cannot be offered for technical reasons, the following recommendations have to be observed:

Privacy Policy and Transparency
PTAs or transport companies using e-ticketing systems should provide data subjects with unambiguous information on the processing of personal data which they carry out. Data subjects should be in a position to easily understand all the specific purposes sought by the companies, what items of personal information concerning them are collected and stored, and how such information is used.

Data Minimization and Retention Period
As regards, in particular, processing of the data concerning users' movements, the information systems of transport companies should be designed and implemented by prioritizing the use of anonymous data. If (directly or indirectly) identifiable information is used, this information should be stored for the shortest possible period (and erased automatically thereafter), and account should be taken of the lawful purposes to be achieved via the processing – as a rule, the information in question should not be retained for longer than a few days after being stored.

Security
Security for accessing personal data should include an audit system to prohibit the misuse of information. Transport companies should ensure that the privacy of

registered users is guaranteed when making their databases accessible to partners or even their own employees.

Marketing
A PTA or transport company should obtain the free and informed prior consent of customers for the use of personal data for its own marketing purposes or associated partner's usage of information for unsolicited marketing towards the traveller. This consent should be distinct from the acceptance of the general contractual obligations.

Proof of Payment
As far as proof of payment for individual journeys is required e.g. for refunds or tax allowances, privacy-friendly solutions should be offered.

Code of Conduct
The adoption of a privacy code of conduct should be encouraged. As regards, in particular, processing of the data concerning users' movements, the information systems of transportation companies should be designed and implemented by prioritizing the use of anonymous data.

System Design
System design should be such as to separate the personal information from travel information (two-component model). Central storage should be reserved for aggregate data and/or anonymous transactions. The Cardholder should be able to control information concerning his use of the card.

Arbeitspapier

Datenschutz bei der Verbreitung digitaler Medieninhalte und beim digitalen Fernsehen

Entwicklungszusammenhang

Das Fernsehen hat im letzten Jahrzehnt fundamentale Veränderungen erfahren.

Die erste Entwicklung – der Übergang vom **analogen** zum **digitalen Fernsehen** – war überwiegend eine Umrüstung von analoger zu digitaler Erfassung, Aufnahme, Übertragung und Wiedergabe. Sie bewirkte besseren Ton, bessere Bilder, mehr Kanäle und mehr Auswahl, veränderte aber nicht fundamental Form und Funktion der klassischen Ausstrahlung von Fernsehen.

Die zweite Entwicklung – die Auslieferung von Fernsehen und anderen Audio- und Videodiensten als digitale Signale **über Breitbanddatennetzwerke** – verändert die Bedingungen der Medienproduktion, -verteilung und -inanspruchnahme in signifikanter Weise. Sie beinhaltet die Konvergenz der Kommunikations-, Computer- und Massenmediensektoren in einem einzigen, interaktiven Netzwerk – **Konvergenz der Netzwerke** – und die Einführung einer zunehmenden Anzahl von statischen oder mobilen Endgeräten, die in der Lage sind, gleichmäßig mit diesen drei Sektoren zu interagieren – **Divergenz der Endgeräte**. Sie beinhaltet auch die Einführung neuer Navigationsparadigmen, die durch neue Werkzeuge und Dienste, wie Video-Suchmaschinen, peer-to-peer-Verteilung usw. den Zugriff auf eine explosiv wachsende Anzahl von Bildmedien gestattet – **Divergenz der Inhalte**. Schließlich ermöglicht sie potenziell die Erhebung und Verarbeitung personenbezogener Daten aus verschiedenen Quellen, z. B. bei Multiple-Play-Diensten.

Zu den wichtigen Folgen dieser zweiten Evolution zählen die Einführung neuer Wege zur Verteilung digitaler Medieninhalte, wie digitales interaktives Fernsehen, IPTV, web-basiertes Fernsehen etc. und die Ersetzung traditioneller set-top-Boxen im Kabelfernsehen durch interaktive, intelligente Geräte. In diesen Systemen können Nutzer einen bestimmten Strom von Videosignalen oder einen Fernsehkanal „on demand" herunterladen, und sie können nicht nur mit dem Inhalt des TV-Programms direkt interagieren, sondern auch mit jeglichem anderen TV-bezogenen Inhalten.

Während das digitale interaktive Fernsehen einen neuen, personalisierten Ansatz beim Fernsehen darstellt – jedermann zu beliebigen Zeitpunkten an beliebigen Orten und auf beliebigen Endgeräten alle möglichen Inhalte zur Verfügung zu stellen – und neue Dienste wie „T-Commerce[1]", Video-on-demand, Home-Banking und Fernstudium ermöglicht, führt es auch zu neuen Gefährdungen, insbesondere im Hinblick auf den Schutz der Privatsphäre der Nutzer.

Die neuen interaktiven, digitalen Fernsehsysteme nutzen in den meisten Fällen eine versiegelte „Black-Box", die von den Anbietern kontrolliert werden und dem Nutzer wenig oder überhaupt keine Kontrolle ermöglichen. Es handelt sich um geschlossene Systeme und es ist selbst für fortgeschrittene Nutzer schwierig, wenn nicht unmöglich, herauszufinden, was diese Systeme tun.

Eine der wichtigsten Gefahren, die durch diese neuen Arten der Verteilung digitaler Medieninhalte entstehen, ist die Möglichkeit, die emotionale Kraft des Fernsehens (Menschen, die sich zuhause entspannen, neigen eher zu offenen unbefangenen Reaktionen mit der Transaktions-orientierten Macht des Internet (Data Mining, Nutzer-Modellierung, intelligente Agenten etc.) zu kombinieren,

[1] Fernseh-basierter Geschäftsverkehr

um hinreichend individualisierte, personalisierte Informationen über jeden Nutzer zu sammeln, um seine Seherfahrungen umgehend daran anzupassen und sogar sein Verhalten zu verändern.

Wenn der Fernsehdienst von einem Internetserviceprovider im Rahmen eines Triple- oder Quadruple-Play-Dienstes angeboten wird, wird das Fernsehprogramm entweder auf einem Fernsehgerät oder einem Personalcomputer angezeigt. In beiden Fällen kann der Kanal „on demand" abgerufen werden (wenn der Nutzer einen Kanal wählt) und der Anbieter kann daher präzise bestimmen, welcher Nutzer ein Programm zu einem bestimmten Zeitpunkt ansieht. Im Falle des Web-TV, bei dem die Inhalte über eine Website angeboten werden, wird der Videodatenstrom ebenfalls „on demand" heruntergeladen; personenbezogene Daten können teilweise wohl durch den Betreiber der Website als auch durch den Internetserviceprovider erhoben und gespeichert werden, der dem Nutzer den Internet-Zugang anbietet[2]. Schließlich erlauben einige Systeme einzelnen Nutzern sogar das Heraufladen eigener Inhalte auf eine Video-on-demand-Plattform (wo andere Nutzer auf sie zugreifen können), oder Nutzer können auch ihre eigenen Bilddaten live in einem speziellen Video-on-demand-Fernsehkanal senden.

Empfehlungen und Bekräftigung fundamentaler Prinzipien

Die Arbeitsgruppe ist insbesondere unter Berücksichtigung der Bedeutung der neuen Möglichkeiten digitalen Medienkonsums in jedermanns täglichen Leben und dessen führender Bedeutung für die Gesellschaft, die Demokratie, die Bildung und Kultur als ein kultureller Dienst, der den freien Zugang zu Informationen garantiert sowie Meinungsvielfalt und Medienpluralismus, und in Erwägung, dass andererseits riesige Mengen sehr sensibler Informationen durch die Registrierung von Nutzungsgewohnheiten gesammelt werden können, der Auffassung, dass:

1. Die Möglichkeit zur anonymen Nutzung des digitalen Fernsehens erhalten bleiben muss. Anonyme Zahlungsmethoden (z. B. durch vorausbezahlte Karten) sollten wenigstens als eine Möglichkeit und ohne zusätzliche Kosten angeboten werden. Informationssysteme (Geräte, Programme und deren Organisation), die für die Verbreitung digitalen Fernsehens genutzt werden, müssen

[2] Darüber hinaus können personenbezogene Daten von der Inhalte-Industrie mittels eines „broadcast flag" erhoben und gespeichert werden, wie man es in den Vereinigten Staaten von Amerika einzuführen versucht hat, und das möglicherweise auch in anderen Ländern erwogen wird. In diesem System sind maschinenlesbare Daten in das Fernsehsignal eingebettet, um die Weiterverbreitung von Inhalten zu verhindern, die urheberrechtlichen Beschränkungen unterliegen. Datenschutzbedenken können entstehen, wenn Technologien zum digitalen Rechte-Management die Nutzung von Inhalten überwachten und mögliche Urheberrechtsverstöße eines Einzelnen an den Inhalteanbieter zurückmelden (vgl. auch den Gemeinsamen Standpunkt der Arbeitsgruppe zu Datenschutz- und Urheberrechts-Management, angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000 in Rethymnon/Kreta; http://www.datenschutz-berlin.de/attachments/233/co_de.pdf).

so entworfen, entwickelt und konfiguriert werden, dass sie Anonymität oder Minimierung der Nutzung personenbezogener Daten befördern und sicherstellen. Zu diesem Zweck sollte eine Vorabkontrolle durchgeführt werden.

2. Wenn personenbezogene Daten gespeichert werden, so darf dies nur für legitime Zwecke geschehen und der Umfang der Daten und die Mechanismen, die zu ihrer Verarbeitung implementiert werden, müssen relevant und nicht unverhältnismäßig im Hinblick auf die zu erreichenden Zwecke sein. Die Eröffnung von Wahlmöglichkeiten für den Einzelnen im Hinblick auf Inhalte sollte nicht unvermeidbar mit ihrer Identifizierung einhergehen.

3. Anbieter digitalen Fernsehens sollten die Zuschauer im Vorhinein über die genauen Zwecke der Speicherung und Verarbeitung personenbezogener Daten informieren, sowie über die Arten der gespeicherten Daten, den Ort und die Dauer der Speicherung.

4. Die Verarbeitung von Nutzerprofilen sollte die vorherige, informierte Einwilligung der Betroffenen voraussetzen („opt in“). Insbesondere sollte die Übermittlung von Zuschauerdaten oder -profilen durch Anbieter digitalen Fernsehens an Dritte (z. B. zu Werbezwecken) nur mit der freiwilligen und informierten Einwilligung der Betroffenen erfolgen. Diese Einwilligung sollte sich von der Zustimmung zu allgemeinen Geschäftsbedingungen des digitalen Fernsehdienstes unterscheiden. Die Zuschauer sollten das Recht haben, ihre Einwilligung jederzeit mit Wirkung für die Zukunft zurückzuziehen.

5. Zuschauer sollten – vorzugsweise kostenfrei – das Recht auf Auskunft, Überprüfung und – wo notwendig – Berichtigung aller ihrer personenbezogenen Daten haben, einschließlich ihrer bei Anbietern von digitalem Fernsehen gespeicherten Profile.

6. Gespeicherte personenbezogene Daten müssen durch angemessene Sicherheitsmaßnahmen geschützt werden.

7. Die Überprüfung der Einhaltung von Datenschutzbestimmungen durch unabhängige Einrichtungen ist unerlässlich.

Working Paper Privacy Issues in the Distribution of Digital Media Content and Digital Television

Evolution of the context

Television has undergone some fundamental changes in the last decade.

The first evolution – the passage from **analogue television** to **digital television** – was mainly a conversion from analogue to digital acquisition, recording, transmission and reproduction. It provided better sound, better pictures, more channels and more choice but did not change fundamentally the form and function of the classical broadcast television.

The second evolution – the delivery of television and other audio and video services as digital signals **over broadband data networks** – significantly changes the patterns of media production, distribution and consumption. It involves the convergence of communications, computers and mass media sectors into a unique and interactive network – **the convergence of networks** – and the appearance of an increasing number of static or portable media devices able to equally interact with those three sectors – **the divergence of devices**. It also involves the introduction of new navigation paradigms allowing to access, by means of new tools or services like video search engines, peer-to-peer distribution, etc., an explosive growth of available video media – **the divergence of contents**. Finally, it potentially allows for the collection and processing of personal data gathered from different sources, for example in multiple-play services.

Important consequences of this second evolution are the introduction of new ways of distribution of digital media content, like digital interactive television**,** IPTV, web-based TV etc., and the replacement of the traditional cable TV set-top box by an interactive intelligent device. In these systems, users may download a specific video stream or TV channel on demand, and they may interact directly not only with TV program content but also with any other TV related contents.

While digital interactive television presents a new personalized approach to television – to provide anybody, anything, anytime, anywhere and on any device – and allows new services like T-Commerce[1], video-on-demand, home-banking and distance learning, it also introduces new threats, especially with respect to the protection of privacy of viewers.

The new digital interactive television systems are generally based on a sealed "black box" controlled by companies giving the user little or no control. Systems

[1] Television-based Commerce

are closed and it is difficult, if not impossible, even for advanced users to identify what the system is doing.

One of the major threats introduced by these new ways of distribution of digital media content is the possibility to combine the emotional power of television (people relaxing at home more open to react openly without any inhibition) with the transactional power of the Internet (data mining, user modeling, intelligent agents, etc.) to gather sufficiently individualized personalized information about any viewer to adapt immediately and accordingly his viewing experience and even to modify his behavior.

When the television service is offered by an ISP within a triple- or quadruple-play service, the TV program is either viewed on a TV or on a PC. In both cases, the channel may be retrieved on demand (when the user selects the channel) and the provider can therefore identify precisely which user is watching a program at a given moment. Similarly, in the case of WebTV, where the content is provided via a website, the video stream is downloaded on demand; personal data can potentially be collected by the website operator, and also by the ISP providing the internet connectivity to the user[2]. Finally, some systems even allow individual users to upload their own content on a video on demand platform (where it can be accessed by other users), or users may also broadcast their own live video streams on a dedicated VoD TV channel.

Recommendations and recall of fundamental principles

The Working Group, particularly aware of the significance of new ways of digital media consumption in everybody's daily life and its leading importance for societies, democracy education and culture as cultural service ensuring freedom of information, diversity of opinion and media pluralism, and considering on the other hand the huge amount of very sensitive information that can be gathered by registering the users habits, considers that:

1. The possibility of anonymous use of digital television must be maintained. Anonymous payment methods (e.g. prepaid cards) should be offered at least as an option at no additional cost. Information systems (organisation, hardware, software) set up to deliver digital television have to be designed, built and configured to promote and assure anonymity or minimization of the use of

[2] In addition, personal information may be collected by the content industry under a "broadcast flag" regime, which the United States attempted to implement and may be pursued in other countries. In this system digital television signals are embedded with machine readable data to prevent re-distribution of copyrighted content. Privacy concerns can arise when digital rights management technology tracks use of content and reports back to the content provider on an individual's possible copyright infringement (cf. also the Common Position of the Working Group on Privacy and Copyright Management adopted at the 27th Meeting of the Working Group on 4-5 May 2000 in Rethymnon / Crete; http://www.datenschutz-berlin.de/attachments/234/co_en.pdf).

personal data. To this end, a privacy impact assessment should be performed in advance.

2. If personal data are collected, it may only be for legitimate purposes, and the amount of data and the mechanisms implemented to process them have to be relevant and not excessive in respect of the purpose to be achieved. Allowing individuals choice of content should not inevitably require them to be identified.

3. Digital television providers should notify viewers beforehand about the exact purposes of the personal data collection and processing, the type of data collected, the place and duration of storage.

4. The processing of viewers profiles should require their informed prior consent ("opt in"). Specifically, the communication of viewers' data or profiles by digital television providers to a third party (e.g. for marketing purposes) may only be carried out with the free and informed consent of the data subject. This consent should be distinct from the acceptance of the general contractual conditions of the digital television service. Viewers should have a right to withdraw their consent at any time with effect for the future.

5. Viewers should have the right to access, inspect and correct if necessary, preferably free of charge, all their personal data, including their profiles stored by digital television providers.

6. Collected personal data have to be protected by adequate security measures.

7. Verification of privacy compliance by independent bodies is essential.

2008

43. Sitzung, 3. und 4. März 2008, Rom, Italien

Empfehlung zur Umsetzung und Anwendung der Europaratskonvention Nr. 185 zur Computerkriminalität („Budapest Konvention")

Die Budapest Konvention von 2001 zur Computerkriminalität ist ein wesentliches Werkzeug zur internationalen Kooperation mit dem Ziel der Harmonisierung von Straftatbeständen, Strafverfahren und der gerichtlichen und polizeilichen Zusammenarbeit;

In Erwägung, dass verschiedenen Regelungen der Konvention und das dazugehörige Protokoll, wie im Jahr 2003 unterschrieben, direkten Einfluss auf die Verarbeitung personenbezogener Daten haben und dass es wichtig ist, Datenschutzprinzipien bei der Ratifizierung und Umsetzung dieser Bestimmungen in Betracht zu ziehen;

In Erwägung, dass die Bestimmungen der Konvention nicht ausschließlich auf Computerkriminalität anwendbar sind, sondern auch auf die Erhebung von Beweisen in elektronischem Format für jegliche Art von Vergehen, ob mithilfe eines Computersystems begangen oder nicht;

In Erwägung, dass bestimmte Entscheidungen, die auf nationaler Ebene bei der Ratifizierung der Konventionen getroffen werden, auch Effekte auf die internationale Kooperation haben, insbesondere im Hinblick auf Verfahren zur gegenseitigen Hilfeleistung;

In Erwägung, dass auf einige kritische Punkte in diesem Bereich schon während der vorbereitenden Arbeiten für die Konvention hingewiesen worden ist, u. a. durch diese Arbeitsgruppe[1] und durch die Artikel 29-Arbeitsgruppe (Stellungnahme 4/2001 vom 22. März 2001);

in Erwägung, dass verschiedene Länder die Konvention unterschrieben haben, und dass 22 davon sie bereits ratifiziert haben;

EMPFIEHLT die Arbeitsgruppe,

dass besondere Aufmerksamkeit gerichtet werden soll auf alle Implikationen für die Verarbeitung personenbezogener Daten und die Sicherungseinrichtungen für Bürgerrechte in jeglichem Instrumenten zur Ratifizierung der Konvention und des dazugehörigen Protokolls, oder in Verbindung mit deren konkreter Umsetzung durch die zuständigen Untersuchungsbehörden, insbesondere im Hinblick auf Folgendes:

1. **(Verhältnismäßigkeit)** Das Prinzip der Verhältnismäßigkeit, wie es in verschiedenen Artikeln der Konvention niedergelegt ist, sollte bei allen Aktivitäten zur Strafverfolgung, die von den zuständigen Strafverfolgungsbehörden durchgeführt werden (z. B. Untersuchungen, Durchsuchungen, Beschlagnahmen, Festnahmen, Vernehmungen, Suche nach Beweismitteln) immer dann

[1] Vgl. „Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates“ (Berlin, 13./14. September 2000): http://www.datenschutz-berlin.de/attachments/217/cy_de.pfd?1200656839

beachtet werden, wenn das Beweismittel auf einem oder durch ein elektronisches Werkzeug gesammelt werden soll;

2. **(Sicherheitsmaßnahmen für Rechte Dritter)** Immer wenn diese Untersuchungstätigkeit ausgeführt wird, sollte ihr Einfluss auf die Rechte Dritter, die Außenstehende in Bezug auf die untersuchten Fakten sind, mit äußerster Sorgfalt abgeschätzt werden;

3. **(Verantwortung des Unternehmens für Straftaten von Beschäftigten)** In Bezug auf die Umsetzung der Bestimmungen der Konvention über die Verantwortung juristischer Personen (Artikel 12), die eine Verantwortlichkeit juristischer Personen vorsieht, die Einzelpersonen beschäftigen, die für Straftaten verantwortlich gemacht werden, die im Einklang mit der Konvention vorgesehen sind, sollte in Erwägung gezogen werden, die entsprechenden Bestrafungen auch anzuwenden, wenn die betreffenden Straftaten in der nationalen Gesetzgebung zum Schutz personenbezogener Daten enthalten sind;

4. **(„Einfrieren" von Verkehrsdaten)** Die Instrumente zur Umsetzung der Regelungen der Konvention im Hinblick auf die beschleunigte Erhaltung gespeicherter Computerdaten und die teilweise Mitteilung von Verkehrsdaten (Art. 16 und 17) sollte auf der Basis der sorgfältigen Abwägung der Zweckbindungs- und Verhältnismäßigkeitsprinzipien selektiv angewandt werden, wobei auch die Sicherungsmaßnahmen in Betracht gezogen werden sollen, die durch einige Länder festgelegt worden sind, die eine Vorratsdatenspeicherung von Verkehrsdaten für Zwecke der Strafverfolgung vorsehen;

5. **(Nationale Zuständigkeit zur Untersuchung und Aufdeckung von Straftaten)** Um Opfern von Computerkriminalität einen erweiterten Schutz zu bieten, sollte die Ratifizierung der Konvention und/oder jegliche daraus folgenden regulatorischen Änderungen insbesondere auf nationaler Ebene, die Möglichkeit zur Aktualisierung des nationalen Rechts bieten, insbesondere der Bestimmungen, die in den Strafvorschriften und/oder der Strafprozessordnung enthalten sind, um so den Anwendungsbereich der nationalen Gerichtsbarkeit bei der Verfolgung solcher Straftaten auszuweiten, die unbestraft bleiben könnten, wenn die herkömmlichen Standards der Strafgerichtsbarkeit angewandt würden (Art des Verhaltens, Fakten etc.).

Die Arbeitsgruppe erkennt die spezielle Bedeutung internationaler Zusammenarbeit in diesem Bereich an und behält sich vor, weitere Initiativen zu ergreifen, um den Austausch von Informationen, die Überwachung der angemessenen Anwendung der Konvention und des Protokolls, und die weitestmögliche Harmonisierung regulatorischer Ansätze und Umsetzungspraktiken zu fördern.

43rd meeting, 3rd and 4th March 2008, Rome, Italy

Recommendation on the Implementation and Application of the Council of Europe Convention No. 185 on Cybercrime (a.k.a. "Budapest Convention")

Whereas the Budapest Convention of 2001 on cybercrime is a major international co-operation tool with a view to harmonizing criminal offences, investigation procedures, and judicial and police assistance;

Considering that several provisions of the Convention and the relevant Protocol as undersigned in 2003 impact directly on the processing of personal data, and that it is important for data protection principles to be taken into consideration in ratifying and implementing those provisions;

Considering that the provisions of the Convention do not apply exclusively to cybercrime, but also to the collection of evidence in electronic format for whatever type of offence, whether committed by means of a computer system or not; considering that certain decisions made at domestic level in ratifying the Convention produce effects on international co-operation as well, especially with regard to mutual assistance procedures;

Considering that some criticalities in this sector have already been pointed out in the preparatory work to the Convention, inter alia by this Working Group[1], and by the Article 29 Working Party (Opinion no. 4/2001 rendered on 22 March 2001);

Considering that several countries have undersigned the Convention, and twenty-two of them have already ratified it;

RECOMMENDS

That special attention be paid to all the implications for the processing of personal data and the safeguards applying to citizens' rights in any instruments ratifying the Convention and the relevant Protocol, or in connection with the concrete implementation thereof by the competent investigational bodies, in particular with a view to the following:

1. **(Proportionality)** The principle of proportionality, as set out in several articles of the Convention, should be abided by in all criminal investigation activities performed by the competent law enforcement bodies (e.g. inspections,

[1] Cf. "Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe" (Berlin, 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/218/cy_en.pdf

searches, seizure, custody, urgent inquiries, search for evidence) whenever the evidence is to be gathered on and/or by means of electronic tools;

2. **(Safeguards for Third Parties' Rights)** Whenever the said investigations activities are carried out, their impact on the rights vested in third parties that are alien to the facts investigated upon should always be assessed with the utmost care;

3. **(Corporate Liability for Employees' Criminal Offences)** As regards implementation of the provisions in the Convention related to corporate liability (article 12), which envisage the liability of legal persons employing individuals that are held liable for the criminal offences established in accordance with the Convention, consideration should be given to applying the respective punishments also if the criminal offences in question are established under domestic legislation on personal data protection;

4. **("Freezing" of Traffic Data)** The instruments implementing the provisions set out in the Convention with regard to the expedited preservation of stored computer data and the partial disclosure of traffic data (articles 16 and 17) should be applied on the basis of the careful assessment of purpose limitation and proportionality principles as well as in accordance with a selective approach, by also taking account of the safeguards partially laid down by the countries that envisage traffic data retention for law enforcement purposes;

5. **(Countries' Jurisdiction in Investigating and Detecting Criminal Offences)** In order to afford enhanced protection to cybercrime victims, ratification of the Convention and/or any subsequent regulatory amendments, especially at domestic level, should provide an opportunity for updating domestic law, in particular the provisions contained in criminal codes and/or criminal procedure codes, so as to expand the scope of national jurisdiction in prosecuting these offences, which might go unpunished if the conventional standards underlying criminal jurisdiction (type of conduct, facts, etc.) were applied.

The Working Group recognises the special importance of international co-operation in this area and reserves the right to undertake further initiatives in order to foster exchanges of information, monitoring of the appropriate application of the Convention and its Protocol, and the widest possible harmonization of regulatory approaches and implementing practices.

Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten

– „Rom Memorandum“ –

Bericht

Hintergrund

„Das Hauptaugenmerk eines sozialen Netzwerkdienstes ist auf die Bildung und Bestätigung von sozialen Beziehungen im Online-Bereich von Menschen gerichtet, die Interessen und Aktivitäten teilen, oder die an der Erkundung von Interessen und Aktivitäten anderer interessiert sind, und die Nutzung von Software voraussetzt. Die meisten Dienste sind im Wesentlichen webbasiert und bestehen in einer Ansammlung unterschiedlicher Möglichkeiten für Nutzer, zu interagieren [...][1]. Insbesondere ermöglichen viele populäre Websites eine Interaktion mit anderen Nutzern (auf der Basis von selbstgenerierten persönlichen Profilen[2].

Das Aufkommen und die ständig wachsende Popularität sozialer Netzwerkdienste kündigt eine grundlegende Veränderung in Bezug auf die Art und Weise an, wie personenbezogene Daten großer Bevölkerungsgruppen in aller Welt mehr oder weniger öffentlich verfügbar werden. Diese Dienste sind in den letzten Jahren unglaublich populär geworden, insbesondere bei jungen Leuten. Sie werden aber auch zunehmend zum Beispiel im beruflichen Kontext oder für Senioren angeboten.

Die Herausforderungen, die soziale Netzwerkdienste stellen, sind auf der einen Seite nur eine weitere Variation der fundamentalen Veränderung, die die Entwicklungen des Internet in den 90er Jahren des letzten Jahrhunderts mit sich gebracht haben, in dem – unter anderem – Zeit und Raum bei der Veröffentlichung von Informationen und bei Echtzeitkommunikation aufgehoben wurden, und durch die Verwischung der Trennlinie zwischen Diensteanbietern (Autoren) einerseits und Nutzern/Konsumenten (Lesern) auf der anderen Seite.

Gleichzeitig scheinen soziale Netzwerkdienste die Grenzen dessen zu verändern, was gesellschaftlich als die Privatsphäre von Personen gesehen wird: Personenbezogene Daten über Einzelne werden öffentlich (und global) in einer nie vorher da gewesenen Weise und Menge[3] verfügbar, insbesondere riesige Mengen digitaler

[1] zitiert aus Wikipedia; http://en.wikipedia.org/wiki/Social_network_service [abgerufen am 5. Februar 2008]

[2] Dieser Bericht beschäftigt sich nicht mit Chat, Blogging und Bewertungsplattformen

[3] Ein deutscher Wissenschaftler hat kürzlich in einer Auswahl populärer sozialer Netzwerkdienste ungefähr 120 einzelne persönliche Attribute identifiziert, die in Nutzerprofilen sozialer Netzwerkdienste enthalten sind, wie z. B. Name, Privatadresse, Lieblingsfilme, -bücher und –musik usw., wie auch politische Ansichten und sogar sexuelle Vorlieben. Vgl. „Berliner Morgenpost“ vom 23. Januar 2008, S. 9: „Mehr Informationen als die Stasi“; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html.

Bilder und Videos. Im Hinblick auf den Schutz der Privatsphäre könnte eine der grundlegendsten Herausforderungen in der Tatsache gesehen werden, dass die meisten der personenbezogenen Informationen, die in sozialen Netzwerkdiensten publiziert werden, auf Initiative der Nutzer selbst und mit ihrer Einwilligung veröffentlicht werden. Während die „traditionelle" Datenschutzgesetzgebung sich mit der Definition von Regeln zum Schutz der Bürger gegen unfaire oder unverhältnismäßige Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdienste), und von Unternehmen beschäftigt, gibt es nur sehr wenige Regelungen zur Veröffentlichung personenbezogener Daten auf Initiative der Betroffenen selbst, weil dies vor der Entwicklung sozialer Netzwerkdienste weder in der „Offline-Welt" noch im Internet ein großes Problem darstellte. Außerdem ist die Verarbeitung personenbezogener Daten aus öffentlichen Quellen traditionell in der Datenschutzgesetzgebung privilegiert.

Gleichzeitig ist eine neue Generation von Nutzern entstanden: Die erste Generation, die aufgewachsen ist, während das Internet bereits existierte. Diese „digitalen Eingeborenen"[4] haben ihre eigene Art der Nutzung von Internet-Diensten entwickelt, und eigene Ansichten darüber, was sie als der privat- bzw. der öffentlichen Sphäre zugehörig empfinden. Darüber hinaus könnten sie – da die meisten von ihnen im Teenager-Alter sind – eher bereit seien, Datenschutzrisiken einzugehen, als die älteren „digitalen Einwanderer". Generell scheint es, als seien jüngere Leute eher zur Veröffentlichung (manchmal intimer) Einzelheiten über ihr Leben im Internet bereit.

Gesetzgeber, Datenschutzbehörden wie auch Anbieter sozialer Netzwerkdienste sind mit einer Situation konfrontiert, die kein sichtbares Beispiel in der Vergangenheit hat. Während soziale Netzwerkdienste eine neue Bandbreite von Möglichkeiten für die Kommunikation und den Austausch von allen Arten von Informationen in Echtzeit bieten, kann die Nutzung solcher Dienste auch zu Gefährdungen der Privatsphäre der Nutzer (und anderer Bürger, die nicht einmal Teilnehmer an sozialen Netzwerkdiensten sind) führen.

Datenschutz- und Datensicherheitsrisiken

Die Ausbreitung sozialer Netzwerkdienste hat gerade erst begonnen. Während es bereits jetzt möglich ist, einige Risiken zu identifizieren, die mit dem Angebot und der Nutzung solcher Dienste verbunden sind, ist es sehr wahrscheinlich, dass wir gegenwärtig nur die Spitze des Eisbergs sehen, und dass sich in der Zukunft neue Nutzungen – und damit auch neue Risiken – entwickeln. Insbe-

[4] Dieser Begriff wird Marc Prensky zugeschrieben, einem amerikanischen Redner, Autor, Berater und Spieledesigner im Bereich Ausbildung und Bildung. Vgl. z. B. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [abgerufen am 5. Februar 2008]

sondere werden neue Nutzungsformen für die in Nutzerprofilen enthaltenen personenbezogenen Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdiensten[5]), wie auch durch den privaten Sektor, entwickelt werden.

Die folgende Liste von Risiken stellt nur eine Momentaufnahme dar, die möglicherweise mit der Weiterentwicklung sozialer Netzwerkdienste überarbeitet und aktualisiert werden muss.

Risiken in Verbindung mit der Nutzung sozialer Netzwerke, die bisher identifiziert worden sind, schließen die Folgenden ein:

1. *Im Internet gibt es kein Vergessen:* Die Idee des Vergessens ist im Internet nicht existent. Wenn Daten einmal publiziert sind, können sie dort sozusagen „bis in alle Ewigkeit" gespeichert bleiben – sogar dann, wenn der Betroffene sie von der ursprünglichen Website gelöscht hat, könnten Kopien bei Dritten existieren (einschließlich Archivdienste und die „Cache-Funktion", die von einem bekannten Suchmaschinenanbieter angeboten wird). Außerdem weigern sich einige Diensteanbieter, auf Nutzeranforderungen zur Löschung von Daten, und insbesondere von kompletten Profilen schnell (oder sogar überhaupt) zu reagieren.

2. *Der irreführende Begriff der „Gemeinschaft":* Viele Diensteanbieter geben an, dass sie Kommunikationsstrukturen aus der „realen Welt" in den Cyberspace übertragen. Eine häufige Aussage ist, es sei sicher, (personenbezogene) Daten auf diesen Plattformen zu veröffentlichen, weil es lediglich der Weitergabe an Informationen an Freunde (wie früher im direkten Kontakt) gleiche. Eine genauere Betrachtung von Eigenschaften einiger dieser Dienste bringt jedoch zutage, dass diese Parallele einige Schwächen hat, einschließlich dessen, dass der Begriff des „Freundes" im Cyberspace in vielen Fällen grundlegend von der hergebrachten Idee von Freundschaft abweicht, und dass eine Gemeinschaft sehr groß sein kann[6]. Wenn die Nutzer nicht offen darüber informiert werden, wie ihre Profilinformationen weitergegeben werden und wie sie diese Weitergabe kontrollieren können, könnten sie durch die

[5] Bereits jetzt scheinen Geheimdienste in den Vereinigten Staaten von Amerika (insbesondere das „Open Source Center", eine Dienststelle, die dem US-amerikanischen „Director of National Intelligence" zugeordnet ist) Daten aus sog. „öffentlichen Quellen" zu nutzen, die anscheinend unter anderem YouTube, aber auch soziale Mediendienste wie Myspace und blogs einschließen; vgl. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html [abgerufen am 7. Februar 2008]

[6] Während einige Diensteanbieter versucht haben, begrenzte Bereiche innerhalb ihrer Dienste zu schaffen, um den Nutzern mehr Kontrolle darüber zu geben, wie sie ihre (personenbezogenen) Daten weitergeben, machen andere solche Informationen oder Teile davon einem größeren Publikum verfügbar, das in manchen Fällen in der gesamten Gemeinschaft bestehen kann – und damit in Millionen von völlig Fremden: „Zwar bleibt es unter uns", aber „wir" können durchaus mehr als 50 Millionen seien.

Idee der „Gemeinschaft“, wie sie oben beschrieben ist, dazu verführt werden, gedankenlos personenbezogene Daten weiterzugeben, die sie sonst nicht weitergeben würden. Schon die Namensgebung mancher dieser Plattformen (z. B. „MySpace“) erzeugt die Illusion von Intimität im Internet.

3. *„Kostenlos“ ist vielleicht nicht „umsonst“,* wenn Nutzer vieler sozialer Netzwerke tatsächlich mit der zweckfremden Nutzung ihrer persönlichen Profildaten durch die Diensteanbieter „bezahlen“, z. B. für (zielgerichtete) Werbung.

4. *Die Speicherung von Verkehrsdaten durch Anbieter sozialer Netzwerkdienste,* die technisch in der Lage sind, jede einzelne Bewegung eines Nutzers auf ihrer Website zu speichern; die eventuelle Weitergabe personenbezogener (Verkehrs-) Daten (einschließlich der IP-Adressen von Nutzern, die in manchen Fällen zusätzlich auch Aufenthaltsinformationen darstellen können) an-Dritte (z. B. für Werbung oder sogar zielgerichtete Werbung). Es ist zu beachten, dass die Daten in vielen Rechtssystemen auch an Strafverfolgungsbehörden und/oder (nationale) Geheimdienste auf deren Verlangen weitergegeben werden müssen, unter Umständen sogar einschließlich ausländischer Stellen im Einklang mit existierenden Regelungen zur internationalen Kooperation.

5. *Die wachsende Notwendigkeit, Dienste zu refinanzieren und Gewinne zu erzielen, könnte die Erhebung, Verarbeitung und Nutzung von Daten der Nutzer weiter anheizen,* wenn und soweit diese den einzigen Vermögenswert der Anbieter sozialer Netzwerkdienste darstellten. Soziale Netzwerkwebseiten sind nicht – wie vielleicht der Ausdruck „sozial“ nahe legen könnte – öffentliche Versorgungsbetriebe. Gleichzeitig wird Web 2.0 als Ganzes „erwachsen“ und es gibt einen Wechsel von startups, die manchmal von Studentengruppen mit weniger finanziellen Interessen geführt werden, zu großen internationalen Unternehmen, die sich an diesem Markt beteiligen. Dies hat zu einer teilweisen Veränderung der Spielregeln geführt, weil viele dieser Unternehmen, die an nationalen Aktienbörsen notiert sind, unter einem extremen Druck ihrer Investoren stehen, Gewinne zu erzielen und zu maximieren. Weil für viele Anbieter sozialer Netzwerke die Daten in den Nutzerprofilen und die Nutzeranzahl (in Kombination mit der Nutzungshäufigkeit) den einzigen wirklichen Verkehrswert darstellt, den diese Unternehmen haben, könnte dies zu zusätzlichen Gefahren der unverhältnismäßigen Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Nutzer führen. Dabei ist auch zu beachten, dass viele Anbieter sozialer Netzwerke das Konzept der Externalisierung von Kosten des Datenschutzes hin zu den Nutzern verfolgen[7].

[7] vgl. die Rede von John Lawford (Canadian Public Interest Advocacy Center) beim OECD-Canada Technology Foresight Forum “Confidence, privacy and security” am 3. Oktober 2007; http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf [abgerufen am 6. Februar 2008], S. 35

6. *Es könnten mehr personenbezogene Informationen weitergegeben werden als man denkt:* So könnten z. B. Fotos zu universellen biometrischen Identifikatoren innerhalb eines Netzwerks oder sogar über Netzwerke hinweg werden. Software zur Gesichtserkennung ist in den letzten Jahren dramatisch verbessert werden und wird in der Zukunft sogar noch „bessere" Ergebnisse erzielen. Es ist zu beachten, dass, wenn einmal ein Name zu einem Bild hinzugefügt werden kann, dies auch die Privatsphäre und Sicherheit anderer, möglicherweise pseudonymer oder sogar anonymer Nutzerprofile in Gefahr bringen kann (z. B. bei Profilen in Kontaktanzeigen, die normalerweise aus einem Bild und Profilinformationen bestehen, aber nicht den wirklichen Namen des Betroffenen veröffentlichen). Die Europäische Netzwerks- und Informationssicherheitsagentur weist außerdem auf eine in der Entwicklung befindliche Technologie namens „content based image retrieval" (CBIR) hin, die weitere Möglichkeiten zur Lokalisierung von Nutzern durch Vergleich identifizierender Bestandteile eines Ortes mit Aufenthaltsinformationen in einer Datenbank ermöglicht[8] (z. B. ein Bild, das in einem Raum an der Wand hängt, oder ein abgebildetes Gebäude). Darüber hinaus führen „soziale Graphen"-Funktionen, die bei vielen sozialen Netzwerkdiensten beliebt sind, zur Offenlegung von Daten über die Beziehungen zwischen verschiedenen Nutzern.

7. *Missbrauch von Profildaten durch Dritte:* Dies ist möglicherweise das wichtigste Bedrohungspotenzial für personenbezogene Daten, die in Nutzerprofilen sozialer Netzwerkdienste enthalten sind. Abhängig davon, ob (Standard-) Einstellmöglichkeiten zum Datenschutz existieren und ob und wie diese von den Betroffenen genutzt werden, wie auch von der technischen Sicherheit eines sozialen Netzwerkdienstes, werden Profilinformationen, einschließlich Bildern (die den Betroffenen selbst, aber auch andere Personen abbilden können) im schlimmsten Fall der gesamten Nutzergemeinschaft zugänglich gemacht. Gleichzeitig existieren gegenwärtig nur sehr wenige Schutzvorkehrungen gegen das Kopieren von Daten jeglicher Art aus Nutzerprofilen und deren Nutzung zum Aufbau von Persönlichkeitsprofilen, und/oder deren Wiederveröffentlichung außerhalb des sozialen Netzwerkdienstes[9].

   Aber sogar die „normale" Nutzung von Profildaten kann das informationelle Selbstbestimmungsrecht von Nutzern und beispielsweise auch ihre beruf-

[8] vgl. ENISA Position Paper No. 1: „Security Issues and Recommendations for Online Social Netzworks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[9] Dabei ist zu beachten, dass einige soziale Netzwerkdienste es Suchmaschinen gestatten, Daten ihrer Nutzer zu durchsuchen und dass in letzter Zeit Suchmachinendienste entstanden sind, die auf das Angebot von Persönlichkeitsprofilen spezialisiert sind, die aus verschiedenen Quellen zusammengestellt werden. Andererseits scheinen Diensteanbieter gegenwärtig wenig oder sogar überhaupt keine Kontrolle über die Handlungen von „Spidern" auf ihren Websites zu haben, die das „robots.txt"-Protokoll nicht respektieren.

lichen Perspektiven in gravierender Weise beeinträchtigen[10]: Ein Beispiel, das öffentliche Aufmerksamkeit erlangt hat, ist die Durchsuchung von Nutzerprofilen von Bewerbern oder Angestellten durch Personalmanager, die sich als Standardprozedur zu entwickeln scheint: Presseberichten zufolge geben bereits heute ein Drittel aller Personalverantwortlichen an, für ihre Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. zur Überprüfung und/oder Vervollständigung von Bewerberdaten[11]. Strafverfolgungsbehörden und Geheimdienste (einschließlich solcher aus weniger demokratischen Staaten mit niedrigen Datenschutzstandards) stellen weitere Instanzen dar, die wahrscheinlich Nutzen aus diesen Quellen ziehen werden[12]. Darüber hinaus stellen einige Anbieter sozialer Netzwerkdienste Nutzerdaten über Programmierschnittstellen Dritten zur Verfügung, so dass diese Daten sich dann unter der Kontrolle dieser Dritten befinden[13].

8. *Die Arbeitsgruppe ist besonders besorgt über* weiter steigende Risiken des Identitätsdiebstahl, die durch die breite Verfügbarkeit personenbezogener Daten in Nutzerprofilen und durch die mögliche Übernahme von Profilen durch nicht autorisierte Dritte gefördert werden könnte[14].

9. *Nutzung einer bekanntermaßen unsicheren Infrastruktur:* Viel ist bereits über den Mangel an Sicherheit von Informationssystemen und -netzen einschließlich Internetangeboten geschrieben worden. Zwischenfälle neueren Datums betreffen auch bekannte Anbieter sozialer Netzwerke wie Facebook[15], flickr[16],

[10] „26. April – Eine Frau aus Pennsylvania gibt an, dass ihre Laufbahn als Lehrer durch die Universitätsverwaltung aus dem Gleichgewicht gebracht worden ist, durch unfaire Disziplinarmaßnahmen wegen eines Fotos auf MySpace, das sie mit einem Piratenhut zeigt, wie sie aus einer Plastiktasse trinkt. In einem Bundesgerichtsverfahren gibt [...] an, dass die Millersville Universität sie beschuldigt, für Alkoholkonsum Minderjähriger zu werben, nachdem sie ihr MySpace Foto entdeckt hatten, das mit ‚betrunkener Pirat' beschriftet war". Zitiert aus http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [abgerufen am 11. Februar 2008]. vgl. auch „The Guardian" vom 11. Januar 2008: „Would-be students checked on Facebook"; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html

[11] Vgl. z. B. „Employers Use 'Facebook' and 'MySpace' to Weed Out Applicants"; http://www.wtlv.com/tech/news/news-article.aspx?storyid=644533 [abgerufen am 12. Februar 2008]. Finnland scheint bisher das einzige Land zu sein, das solche Praktiken verbietet.

[12] Andere Beispiele, die sich in der Zukunft entwickeln könnten, könnten auch die Nutzung durch Einwanderungsbehörden bei Auslandsreisen einschließen.

[13] Vgl. z. B. „Facebook API Unilaterally Opts Users Into New Services", von Ryan Singel, 25. Mai 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; vgl. auch Chris Soghoian: „Exclusive: The next Facebook privacy scandal", 23. Januar 2008, http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [abgerufen am 12. Februar 2008]

[14] Vgl. als ein aussagekräftiges Beispiel z. B. die kürzlichen „Natalie"- und „frog"-Experimente, die von der Sicherheitsfirma Sophos durchgeführt worden sind; s. „Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites", August 2007; http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html und "Der Fall 'Natalie'. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites", 21 Januar 2008

[15] Vgl. „Secret Crush Facebook App Installing Adware, Security Firm Charges", 'Wired' vom 3. Januar 2008, http://blog.wired.com/27bstroke6/2008/01/secret-crush-fa.html [abgerufen am 12. Februar 2008]

[16] Vgl. "Phantom Photos: My photos have been replaced with those of another"; http://flickr.com/help/forum/33657/ [abgerufen am 12. Februar 2008]

MySpace[17], Orkut[18] und den deutschen Anbieter „StudiVZ“[19]. Obwohl die Diensteanbieter Maßnahmen zur Verbesserung der Sicherheit ihrer Systeme getroffen haben, gibt es hier immer noch Möglichkeiten zur weiteren Verbesserung. Gleichzeitig ist es wahrscheinlich, dass auch in Zukunft neue Sicherheitslücken auftauchen werden und es ist aufgrund der Komplexität der Softwareanwendungen auf allen Ebenen von Internetdiensten[20] unwahrscheinlich, dass 100%ige Sicherheit jemals realisiert werden kann.

10. *Ungelöste Sicherheitsprobleme von Internetdiensten* tragen zu den Risiken der Nutzung sozialer Netzwerkdienste bei und könnten in bestimmten Fällen solche Risiken verstärken oder zur Entwicklung von spezifischen Spielarten dieser Risiken für soziale Netzwerkdienste führen. Ein kürzlich veröffentlichtes Positionspapier der Europäischen Netzwerk- und Informationssicherheitsagentur (ENISA) benennt u. a. SPAM, cross site scripting, Viren und Würmer, spear-phishing und Phising (spezifisch für soziale Netzwerke), die Infiltrierung von Netzwerken, Profil-Übernahmen und Rufschädigungen durch Identitätsdiebstahl, Stalking, Mobbing und Wirtschaftsspionage (d. h. social engineering-Angriffe unter Nutzung von sozialen Netzwerkdiensten)[21]. Nach Aussage von ENISA stellen Aggregatoren für soziale Netzwerke („social network aggregators“) ein zusätzliches Sicherheitsrisiko dar[22].

11. *Die Einführung von Interoperabilitätsstandards und Anwendungsprogrammierungs-Schnittstellen* (Application Programming Interfaces – API; z. B. „open social“, das von Google im November 2007 vorgestellt wurde), um verschiedene soziale Netzwerkdienste technisch interoperabel zu machen, enthalten zusätzliche neue Risiken: Sie erlauben die automatische Auswertung aller sozialen Netzwerke, die diesen Standard implementieren. Die API liefert buchstäblich die gesamte Funktionalität zur automatischen Auswertung, die auch in der Web-Schnittstelle implementiert ist. Mögliche Anwen-

[17] Vgl. z. B. im Dezember 2006 “MySpace XSS QuickTime Worm”; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708 [abgerufen am 12. Februar 2008]

[18] Vgl. PC World: “Worm Hits Google‘s Orkut” vom 19. Dezember 2007, http://www.pcworld.com/article/id,140653-c,worms/article.html, und SC Magazine US: “Google’s Orkut hit by self-propagating trojan” vom 26. Februar 2008, http://www.scmagazineus.com/Googles-Orkut-hit-by-self-propagating-trojan/article/107312/ [beide abgerufen am 3. März 2008]

[19] vgl. „Datenleck beim StudiVZ? [Update]”; http://www.heise.de/newsticker/meldung/81373/ [abgerufen am 12. Februar 2008]

[20] Außerdem wird der jährliche steile Anstieg der Menge elektronisch gespeicherter Informationen selbst als ein Sicherheitsrisiko angesehen: Bei der letzten RSA Europe Security Conference in London im Jahr 2007 wurde der RSA-Präsident Art Coviello mit der Aussage zitiert, dass allein im Jahr 2006 weltweit 176 Exabytes an Daten generiert worden seien und dass eine solch riesige Menge von Daten aus seiner Sicht nicht verwaltbar sei und nicht effektiv gesichert werden könnte; vgl. das deutsche Computermagazin „iX“, Dezember 2007, S. 22: „Trübe Aussichten: Große Datenmengen verhindern Datensicherheit“; http://www.heise.de/kiosk/archiv/ix/2007/12/022/ [abgerufen am 12. Februar 2008]

[21] ENISA Position Paper No.1: “Security Issues and Recommendations for Online Social Networks”, Oktober 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[22] vgl. ENISA Position Paper No.1 (s. Fußnote 21), S. 12

dungen, die das Potenzial für Rückwirkung auf die Privatsphäre der Nutzer haben (und möglicherweise auch für die Privatsphäre von Nicht-Nutzern, deren Daten Teil eines Nutzerprofils sind) könnten beinhalten: Die globale Analyse von (beruflichen und privaten) Nutzerbeziehungen, die sehr wohl „Grenzen" zwischen verschiedenen Netzwerken überschreiten können, in denen Nutzer in verschiedenen Rollen agieren (z. B. beruflich orientierte gegenüber mehr freizeitorientierten Netzwerken). Interoperabilität könnte auch das Herunterladen und die Verwendung von Profilinformationen und Fotos durch Dritte fördern, sowie die Erstellung von Aufzeichnungen über Veränderungen in Nutzerprofilen (einschließlich des Verfügbarmachens von Informationen, die ein Nutzer aus seinem Profil gelöscht hat).

Empfehlungen

Gestützt auf das oben Gesagte gibt die Arbeitsgruppe die folgenden (vorläufigen) Empfehlungen für Gesetzgeber, Anbieter und Nutzer von sozialen Netzwerkdiensten:

Gesetzgeber

1. *Einführung eines optionalen Rechts auf pseudonyme Nutzung – d. h. in einem sozialen Netzwerkdienst unter einem Pseudonym zu handeln*[23] – wo dies nicht bereits Teil des Regulierungsrahmens ist.

2. *Es muss sichergestellt werden, dass Diensteanbieter in ehrlicher und klarer Weise darlegen, welche Daten für den Basisdienst erforderlich sind, so dass die Nutzer eine informierte Wahl treffen können, ob sie den Dienst in Anspruch nehmen wollen,* und dass Nutzer jegliche zweckfremde Nutzung (wenigstens durch Widerspruch) ablehnen können, insbesondere zum Zwecke von (zielgerichteter) Werbung. Dabei ist zu beachten, dass hinsichtlich der Einwilligung von Minderjährigen besondere Probleme bestehen[24].

3. *Einführung einer Verpflichtung für Anbieter sozialer Netzwerkdienste zur Benachrichtigung bei Sicherheitsvorfällen.* Nutzer sind nur dann in der Lage, insbesondere mit den steigenden Risiken von Identitätsdiebstahl umzugehen, wenn sie über jegliche Datensicherheitsvorfälle unterrichtet werden. Eine solche Maßnahme würde gleichzeitig dazu beitragen, ein besseres Bild darüber

[23] „Pseudonyme Nutzung" bedeutet in diesem Kontext das Recht, in einem sozialen Netzwerkdienst unter einem Pseudonym zu handeln, ohne seine „wirkliche" Identität gegenüber anderen Nutzern des Dienstes oder der Öffentlichkeit offenbaren zu müssen, wenn der Nutzer dies wünscht. Abhängig von den konkreten Umständen, kann dies sehr wohl eine Verpflichtung zur Preisgabe der wirklichen Identität gegenüber dem Anbieter eines sozialen Netzwerks bei der Registrierung einschließen.

[24] vgl. das „Arbeitspapier zum Schutz der Privatsphäre von Kindern im Netz: Die Rolle der elterlichen Einwilligung", angenommen bei der 31. Sitzung der Arbeitsgruppe am 26./27. März 2002 in Auckland (Neuseeland); http://www.datenschutz-berlin.de/attachments/204/child_de.pdf?1177661067

zu erhalten, wie gut Unternehmen Nutzerdaten sichern, und ihnen einen zusätzlichen Anreiz liefern, ihre Sicherheitsmaßnahmen weiter zu optimieren.

4. *Überdenken des gegenwärtigen Regulierungsrahmens im Hinblick auf die Verantwortlichkeit* in sozialen Netzwerkdiensten veröffentlichte personenbezogene Daten (insbesondere für personenbezogene Daten Dritter) mit Blick darauf, möglicherweise den Anbietern sozialer Netzwerkdienste ein Mehr an Verantwortlichkeit für personenbezogene Daten auf sozialen Netzwerk-Webseiten zuzuweisen.

5. *Verbesserung der Integration von Datenschutzkenntnissen im Bildungssystem.* So wie die online Veröffentlichung personenbezogener Daten Teil des täglichen Lebens besonders junger Menschen wird, müssen Datenschutz und Instrumente zum informationellen Selbstschutz Teil der Schul-Lehrpläne werden.

Anbieter von sozialen Netzwerkdiensten

Anbieter sollten ein vitales Eigeninteresse an der Datensicherheit und dem Schutz personenbezogener Daten ihrer Nutzer haben. Ein Versäumnis schneller Fortschritte in diesem Bereich könnte zum Verlust des Vertrauens der Nutzer (das bereits jetzt durch kürzliche Datenschutz- und Datensicherheitsvorfälle beträchtlich erschüttert ist) und damit sehr wohl zu einem ökonomischen Rückschlag führen, der mit der Krise vergleichbar ist, die die digitale Wirtschaft in den späten 90er Jahren erschütterte.

1. *Verständliche und offene Informationen der Nutzer* ist eines der bedeutendsten Elemente jeglicher fairen Verarbeitung und Nutzung personenbezogener Daten. Während die Notwendigkeit eines solchen Mechanismus in den meisten nationalen, regionalen und internationalen Regulierungsinstrumenten zum Datenschutz anerkannt ist, muss u. U. die gegenwärtige Form, in der viele Diensteanbieter ihre Nutzer informieren, erneut überdacht werden: Gegenwärtig – und in vielen Fällen im Einklang mit dem existierenden Regulierungsrahmen – stellen Informationen über den Datenschutz einen Teil von manchmal komplizierten und länglichen Vertragsbedingungen des Diensteanbieters dar. Zusätzlich wird manchmal eine Datenschutzinformation angeboten. Manche Diensteanbieter legen nahe, dass der Prozentsatz der Nutzer sehr klein ist[25], die diese Informationen tatsächlich herunterladen. Selbst wenn diese Information dem Nutzer zum Zeitpunkt der Registrierung auf dem Bildschirm angezeigt wird und auf Wunsch des Nutzers auch später abgerufen werden kann, könnten dem Ziel der Information der Nutzer über

[25] Ein Vertreter von Facebook erklärte kürzlich auf einer Konferenz der OECD, dass der Prozentsatz der Nutzer, die eine Datenschutzinformation abrufen, nicht höher als ein Viertel % sein könnte; vgl. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf, S. 33 f [abgerufen am 6. Februar 2008]

mögliche Konsequenzen ihres Handelns während der Nutzung des Dienstes (z. B. bei der Veränderung von Datenschutz-Einstellungen einer Sammlung von Bildern) besser durch eingebaute, kontext-sensitive Funktionen gedient werden, die die angemessene Information auf der Basis der Handlungen der Nutzer liefern.

Die Nutzer sollten insbesondere Informationen über den Regulierungsrahmen enthalten, dem ein Diensteanbieter unterliegt, über ihre Rechte (z. B. auf Auskunft, Berichtigung und Löschung) im Hinblick auf ihre eigenen personenbezogenen Daten und zu dem Geschäftsmodell, das zur Finanzierung des Dienstes angewandt wird. Die Information muss auf die spezifischen Bedürfnisse der jeweiligen Zielgruppe zugeschnitten werden (besonders bei Minderjährigen), damit diese informierte Entscheidungen treffen können.

Die Information der Nutzer sollte sich auch auf den Umgang mit Daten Dritter beziehen: Anbieter sozialer Netzwerkdienste sollten – zusätzlich zur Information ihrer Nutzer über die Art und Weise, wie sie die Daten der Nutzer behandeln – auch über Ge- und Verbote im Hinblick darauf informieren, wie die Nutzer Daten Dritter behandeln dürfen, die in ihren Profilen enthalten sind (z. B. wann die Einwilligung eines Betroffenen vor der Veröffentlichung eingeholt werden muss oder über mögliche Konsequenzen von Regelverstößen). Besonders die riesigen Mengen von Fotos in Nutzerprofilen, auf denen Dritte abgebildet sind (in vielen Fällen sogar versehen mit Hinweisen auf den Namen und/oder das Nutzerprofil des Dritten) spielen in diesem Kontext eine Rolle, weil die gegenwärtigen Praktiken in vielen Fällen nicht mit den existierenden gesetzlichen Rahmen zur Regelung des Rechts am eigenen Bild übereinstimmen.

Freimütige Informationen sollten auch über verbleibende Sicherheitsrisiken gegeben werden und über andere mögliche Konsequenzen der Veröffentlichung personenbezogener Daten in einem Profil, wie auch über den möglichen gesetzmäßigen Zugriff durch Dritte (einschließlich Strafverfolgungsbehörden und Geheimdiensten).

2. *Einführung der Möglichkeit, pseudonyme Profile zu erstellen und zu nutzen, und für deren Nutzung werben.*

3. *Einhaltung von Versprechungen gegenüber den Nutzern:* Eine „conditio sine qua non“ zur Förderung und zum Erhalt des Nutzervertrauens ist die klare und unmissverständliche Information darüber, wie ihre Daten durch den Diensteanbieter genutzt werden, besonders, soweit es die Übermittlung personenbezogener Daten an Dritte betrifft. Bei einigen Diensteanbietern bestehen allerdings gegenwärtig Zweideutigkeiten im Hinblick auf diese Versprechungen. Das bekannteste Beispiel ist die beliebte Aussage „Wir werden Ihre

personenbezogenen Daten niemals an Dritte weitergeben“ in Verbindung mit zielgerichteter Werbung. Während diese Aussage in den Augen des Diensteanbieters formal korrekt sein mag, unterlassen es manche Anbieter, in klarer Weise die Tatsache zu kommunizieren, das z. B. für die Anzeige von Werbeeinblendungen in dem Browser-Fenster eines Nutzers die IP-Adresse dieses Nutzers an einen anderen Diensteanbieter, der den Inhalt der Werbung liefert, weitergegeben werden könnte. Dies geschieht in manchen Fällen gestützt auf Informationen aus dem Profil eines Nutzers, die der Anbieter des sozialen Netzwerkdienstes verarbeitet. Während die Profilinformation selbst möglicherweise tatsächlich nicht an den Werbeanbieter weitergegeben wird, wird sehr wohl die IP-Adresse des Nutzers übermittelt[26] (falls der Anbieter des sozialen Netzwerks nicht z. B. einen Proxy-Mechanismus nutzt, um die IP-Adresse des Nutzers gegenüber dem Werbeanbieter zu verbergen). Einige Anbieter sozialer Netzwerkdienste nehmen irrtümlich an, dass es sich bei IP-Adressen nicht um personenbezogene Daten handelt, während dies in den meisten Rechtsordnungen tatsächlich der Fall ist. Solche Mehrdeutigkeiten können Nutzer irreführen, und eine Erosion des Vertrauens befördern, wenn die Nutzer erfahren, was wirklich passiert. Dies ist weder im Interesse der Nutzer, noch im Interesse des Diensteanbieters. Vergleichbare Probleme existieren hinsichtlich der Nutzung von Cookies.

4. *Datenschutzfreundliche Standardeinstellungen* spielen beim Schutz der Privatsphäre der Nutzer eine Schlüsselrolle: Es ist bekannt, dass nur eine Minderheit von Nutzern Veränderungen an Standardeinstellungen einschließlich der Datenschutzeinstellungen vornimmt, wenn sie sich bei einem Dienst anmelden. Die Herausforderung für die Diensteanbieter liegt dabei darin, Einstellungen zu wählen, die standardmäßig einen hohen Grad an Schutz der Privatsphäre bieten, ohne den Dienst unbenutzbar zu machen. Gleichzeitig ist die Benutzerfreundlichkeit der Einstellmöglichkeiten entscheidend dafür, die Nutzer zu Änderungen zu ermutigen. In jedem Fall sollte die Nicht-Indexierbarkeit von Profilen durch Suchmaschinen als Standard eingestellt sein.

5. *Verbesserung der Nutzerkontrolle über die Nutzung von Profildaten:*

   - *Innerhalb der Gemeinschaft;* z. B. indem die Sichtbarkeit ganzer Profile und von in den Profilen enthaltenen Daten begrenzt werden kann, wie auch die Begrenzung der Sichtbarkeit in Bezug auf Suchfunktionen innerhalb des Netzwerks. Die Kennzeichnung von Fotos (d. h. das Hinzufügen von Links auf existierende Nutzerprofile oder des Namens der abgebildeten Person(en) sollte an die vorherige Einwilligung der Betroffenen gebunden sein.

[26] Abhängig von den Umständen kann der Werbeanbieter sogar in der Lage sein, einige oder die gesamte dahinterliegende Profilinformation auf der Basis der Art der zielgerichteten Werbung, die einem bestimmten Nutzer angezeigt werden soll, zu rekonstruieren.

- *Schaffung von Möglichkeiten, die eine Kontrolle der Nutzer über die Nutzung von Profildaten durch Dritte erlauben – dies ist* unerlässlich, um insbesondere Risiken des Identitätsdiebstahls zu begegnen. Im Augenblick existieren allerdings nur begrenzte Möglichkeiten zur Kontrolle von Informationen, nachdem diese veröffentlicht sind. Die Erfahrungen der Film- und Musikindustrie mit Technologien zur digitalen Rechteverwaltung legt nahe, dass die Möglichkeiten in dieser Hinsicht auch in Zukunft begrenzt bleiben könnten. Trotzdem sollten Diensteanbieter Forschungsaktivitäten in diesem Bereich verstärken: Existierende und möglicherweise vielversprechende Ansätze sind u. a. Forschungsvorhaben zum „semantischen" oder „policy-aware web"[27], die Verschlüsselung von Nutzerprofilen, die dezentrale Speicherung von Nutzerprofilen (z. B. bei den Nutzern selbst), die Nutzung von Wasserzeichen-Technologien für Fotos, die Nutzung von Grafiken anstatt von Text für die Anzeige von Informationen und die Einführung eines Verfallsdatums, das Nutzer für ihre eigenen Profildaten setzen können[28]. Diensteanbieter sollten außerdem danach streben, die zweckfremde Nutzung insbesondere von Bildern zu verhindern, indem sie den Nutzern eine Funktion zur Verfügung stellen, die die Pseudonymisierung oder sogar Anonymisierung von Bildern ermöglicht[29]. Sie sollten darüber hinaus effektive Maßnahmen zur Verhinderung des Durchsuchens und des massenweisen Herunterladens von Profildaten treffen. Insbesondere sollten Nutzerdaten durch (externe) Suchmaschinen nur dann durchsucht werden können, wenn der Nutzer seine ausdrückliche, vorherige und informierte Einwilligung gegeben hat.

- *Ermöglichung der Nutzerkontrolle über die zweckfremde Nutzung von Profil- und Verkehrsdaten;* z. B. für Werbezwecke, als Minimum: ein Widerspruchsrecht für allgemeine Profildaten, eine Einwilligung für sensitive Profildaten (z. B. politische Überzeugungen, sexuelle Orientierungen) und für Verkehrsdaten. Viele existierende Rechtsrahmen enthalten bindende Regelungen für die zweckfremde Nutzung für Werbezwecke, die von Anbietern sozialer Netzwerke eingehalten werden müssen. Sie sollten in Betracht ziehen, die Nutzer selbst darüber entscheiden zu lassen, welche ihrer Profildaten sie für zielgerichtete Werbung genutzt sehen wollen. Zusätzlich sollte die Einführung einer Gebühr nach Wahl des Nutzers als weitere

[27] vgl. z. B. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: "Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web:, E. Ferrari and B. Thuraisingham (Herausgeber), Web and Information Security Idea Group Inc., Hershey, PA (in Erscheinen); http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf , und Sören Preibusch, Bettina Hoser, Seda Gürses und Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [beide abgerufen am 12 Februar 2008].

[28] Vgl. z. B. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. März 2007, S. 40, Punkt 7.2.1

[29] vgl. ENISA Position Paper No. 1: "Security Issues and Recommendations for Online Social Networks", Oktober 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, S. 23

Möglichkeit erwogen werden, um den Dienst dadurch, anstatt durch die Nutzung von Profildaten für Werbezwecke zu finanzieren.

- *Einhaltung der Rechte von Nutzern, wie sie in nationalen, regionalen und internationalen Rechtsrahmen zum Datenschutz anerkannt sind;* einschließlich des Rechts der Betroffenen auf zeitnahe Löschung ihrer Daten (dabei kann es sich auch um ganze Nutzerprofile handeln).

- *Berücksichtigung von Problemen, die im Falle der Übernahme oder des Zusammenschlusses von Unternehmen auftreten kann, die soziale Netzwerkdienste anbieten:* Einführung von Garantien für Nutzer, dass der neue Eigentümer gegenwärtige Datenschutz- (und Datensicherheits-) standards beibehält.

6. *Angemessene Mechanismen zur Behandlung von Beschwerden* sollten eingeführt werden (z. B. das „Einfrieren" angefochtener Informationen, oder von Bildern), wo diese nicht bereits existieren, sowohl für Nutzer sozialer Netzwerke, aber auch in Bezug auf personenbezogene Daten Dritter. Wichtig ist eine zeitnahe Rückmeldung an die Betroffenen. Maßnahmen könnten auch ein Bestrafungsmechanismus für missbräuchliches Verhalten in Bezug auf Profildaten anderer Nutzer und personenbezogene Daten Dritter beinhalten (einschließlich des Ausschlusses von Nutzern von einem Dienst, soweit es angemessen ist).

7. *Verbesserung und Erhaltung der Sicherheit von Informationssystemen.* Nutzung anerkannter Methoden („best practices") bei der Planung, Entwicklung und dem Betrieb sozialer Netzwerk-Anwendungen, einschließlich unabhängiger Zertifizierung.

8. *Entwicklung und/oder weitere Verbesserung von Maßnahmen gegen illegale Aktivitäten wie Spamming und Identitätsdiebstahl.*

9. *Angebot verschlüsselter Verbindungen für die Pflege von Nutzerprofilen, einschließlich gesicherter Anmeldeprozeduren.*

10. *Anbieter sozialer Netzwerke, die in verschiedenen Ländern oder sogar global handeln, sollten die Datenschutzstandards der Länder respektieren, in denen sie ihre Dienste anbieten.*

Nutzer sozialer Netzwerke

1. *Seien Sie vorsichtig.* Denken Sie noch einmal darüber nach, bevor personenbezogene Daten (besonders Name, Adresse oder Telefonnummern) in einem sozialen Netzwerk-Profil veröffentlicht werden. Denken Sie auch darüber nach,

ob Sie mit diesen Informationen oder Bildern in einer Bewerbungssituation konfrontiert werden möchten. Pflegen Sie Ihre Profilinformation. Lernen Sie von Geschäftsführern großer Unternehmen: Diese Personen kennen den Wert ihrer personenbezogenen Daten und kontrollieren sie. Deswegen werden Sie keine großen Mengen personenbezogener Informationen über diese Personen im Netz finden.

2. *Denken Sie noch einmal darüber nach, bevor Sie Ihren echten Namen in einem Profil benutzen.* Nutzen Sie stattdessen ein Pseudonym. Bedenken Sie, dass Sie selbst dann nur begrenzte Kontrollmöglichkeiten darüber haben, wer Sie identifizieren kann, weil Dritte in der Lage sein könnten, ein Pseudonym aufzudecken, besonders auf der Basis von Bildern. Erwägen Sie die Nutzung verschiedener Pseudonyme auf verschiedenen Plattformen.

3. *Respektieren Sie die Privatsphäre anderer.* Seien Sie insbesondere vorsichtig bei der Veröffentlichung personenbezogener Daten über andere (einschließlich Bildern oder sogar Bildern mit Zusatzinformationen) ohne die Einwilligung dieser Person. Bedenken Sie, dass die rechtswidrige Veröffentlichung besonders von Bildern in vielen Rechtsordnungen eine Straftat darstellt.

4. *Informieren Sie sich:* Wer bietet diesen Dienst an? Innerhalb welchen Rechtsrahmens? Gibt es einen adequaten Rechtsrahmen zum Schutz der Privatsphäre? Gibt es eine unabhängige Aufsichtsinstanz (wie z. B. einen Datenschutzbeauftragten), an den Sie sich im Fall von Problemen wenden können? Welche Garantien gibt der Diensteanbieter im Hinblick auf den Umgang mit Ihren personenbezogenen Daten? Ist der Dienst von unabhängigen und vertrauenswürdigen Einrichtungen für einen guten Schutz der Privatsphäre, und für gute Sicherheit zertifiziert worden? Nutzen Sie das Internet, um sich über die Erfahrungen anderer mit den Datenschutz- und Datensicherheitspraktiken eines Ihnen unbekannten Diensteanbieters zu informieren. Nutzen Sie vorhandenes Informationsmaterial von Anbietern sozialer Netzwerke, aber auch unabhängige Quellen wie Datenschutzbehörden[30], und Sicherheitsunternehmen[31].

5. *Nutzen Sie datenschutzfreundliche Profileinstellungen.* Begrenzen Sie die Verfügbarkeit von Informationen soweit wie möglich, insbesondere im Hinblick auf die Indexierung durch Suchmaschinen.

---

[30] vgl. z. B. die Broschüre "when online gets out of line" , die gemeinsam von Facebook und dem Information and Privacy Commissioner von Ontario, Canada, veröffentlicht worden ist; http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf, den Elternratgeber der amerikanischen Federal Trade Commission: "Social Networking Sites: A Parent's Guide"; http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm und "Social Networking Sites: Safety Tips for Tweens and Teens"; http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm [alle abgerufen am 3. März 2008]

[31] vgl. z. B. die von Sophos für Facebook vorgeschlagenen Datenschutzeinstellungen; http://www.sophos.com/security/best-practice/facebook.html

6. *Nutzen Sie andere Identifizierungsdaten* (z. B. Login und Passwort) als diejenigen, die Sie auf anderen Webseiten nutzen (z. B. für E-Mail oder zum Online-Banking).

7. *Nutzen Sie Kontrollmöglichkeiten* im Hinblick darauf, wie ein Diensteanbieter Ihre personenbezogenen Profil- und Verkehrsdaten verarbeitet. Widersprechen Sie beispielsweise der Nutzung für zielgerichtete Werbung.

8. *Achten Sie auf die Aktivitäten Ihrer Kinder im Internet,* insbesondere auf Webseiten sozialer Netzwerke.

Schlussbemerkung

Die Arbeitsgruppe fordert Verbraucherschutz- und Datenschutzorganisationen auf, angemessene Maßnahmen zu treffen, um Regulierer, Diensteanbieter, die Öffentlichkeit und insbesondere junge Menschen[32] auf Risiken für die Privatsphäre in Bezug auf die Nutzung sozialer Netzwerke und verantwortliches Verhalten bezüglich der eigenen personenbezogenen Daten, wie auch der Daten anderer, hinzuweisen.

Die Arbeitsgruppe wird zukünftige Entwicklungen bei sozialen Netzwerkdiensten im Hinblick auf den Schutz der Privatsphäre beobachten und diese Empfehlungen soweit notwendig überarbeiten und aktualisieren.

Report and Guidance on Privacy in Social Network Services

– *"Rome Memorandum"* –

Report

Background

"A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software. Most services are primarily web based and provide a

[32] vgl. z. B. die Kampagne „dubestemmer", die von der norwegischen Datenschutzbehörde gestartet worden ist; http://www.dubestemmer.no/english.php, das "DADUS"-Project der portugiesischen Datenschutzbehörde; http://dadus.cnpd.pt, und die in Fußnote 30 oben aufgeführten Initiativen

collection of various ways for users to interact […]"[1]. Specifically, many popular sites offer means to interact with other subscribers (based on self-generated personal profiles[2]).

The advent and ever increasing popularity of social network services heralds a sea change in the way personal data of large populations of citizens all over the world become more or less publicly available. These services have become incredibly popular in the past years especially with young people. But increasingly such services are also being offered e.g. for professionals and the elderly.

The challenges posed by social network services are on the one hand yet another flavour of the fundamental changes that the introduction of the Internet in the 90s of the past century has brought with it, by – inter alia – abolishing time and space in publishing information and real-time communication, and by blurring the line between service providers (authors) on the one hand and users/consumers (readers) on the other.

At the same time, social networking services seem to be pushing at the boundaries of what societies see as a person's individual space: Personal data about individuals become publicly (and globally) available in an unprecedented way and quantity[3], especially including huge quantities of digital pictures and videos.

With respect to privacy, one of the most fundamental challenges may be seen in the fact that most of the personal information published in social network services is being published at the initiative of the users and based on their consent. While "traditional" privacy regulation is concerned with defining rules to protect citizens against unfair or unproportional processing of personal data by the public administration (including law enforcement and secret services), and businesses, there are only very few rules governing the publication of personal data at the initiative of private individuals, partly because this had not been a major issue in the "offline world", and neither on the Internet before social network services came into being. Furthermore, the processing of personal data from public sources has traditionally been privileged in data protection and privacy legislation.

At the same time, a new generation of users has arrived: The first generation that has been growing up while the Internet already existed. These "digital natives"[4]

[1] Quoted from Wikipedia at http://en.wikipedia.org/wiki/Social_network_service [viewed on 5 February 2008]

[2] This report does not cover chat, blogging, and ranking sites.

[3] A German researcher recently identified in a selection of popular social network services about 120 single personal attributes contained in user profiles in social network services, like for example age, home address, favourite movies, books, music etc., and also including political opinions and even sexual preferences. Cf. „Berliner Morgenpost" of 23 January 2008, S. 9: „Mehr Informationen als die Stasi"; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html (in German language)

[4] A term attributed to Marc Prensky, a US speaker, writer, consultant, and game designer in education and learning. Cf. e.g. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [viewed on 5 February 2008]

have developed their own ways of using Internet services, and of what they see to be private and what belongs to the public sphere. Furthermore they – most of them being in their teens – may be more ready to take privacy risks than the older "digital immigrants". In general, it seems that younger people are more comfortable with publishing (sometimes intimate) details of their lives on the Internet.

Legislators, Data Protection Authorities as well as social network service providers are faced with a situation that has no visible example in the past. While social network services offer a new range of opportunities for communication and real-time exchange of any kind of information, the use of such services can also lead to putting the privacy of its users (and of other citizens not even subscribed to a social network service) at risk.

Risks for Privacy and Security

The surge of social network services has only just begun. While it is possible to identify some risks associated to the provision and use of such services already now, it is very likely that we are at present only looking at the tip of the iceberg, and that new uses – and accordingly new risks – will continue to emerge in the future. Specifically, new uses for the personal data contained in user profiles will be invented by public authorities (including law enforcement and secret services[5]) and by the private sector.

The following list of risks can only represent a snapshot which may need to be revised and updated as social network services develop.

Risks associated to the use of social network services identified up to now include the following:

1. *No oblivion on the Internet:* The notion of oblivion does not exist on the Internet. Data, once published, may stay there literally forever – even when the data subject has deleted them from the "original" site, there may be copies with third parties (including archive services and the "cache" function provided by a well-known search engine provider). Additionally, some service providers refuse to speedily comply (or even to comply at all) with user requests to have data, and especially complete profiles, deleted.

2. *The misleading notion of "community":* Many service providers claim that they are bringing communication structures from the "real" world into cy-

[5] Already now, secret services from the United States (namely the "Open Source Center", a service attached to the US "Director of National Intelligence") seem to be using data from what is called "open sources", which seem to include inter alia YouTube, but also social media like Myspace, and blogs; cf. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html [accessed 7 February 2008]

berspace. A common claim is that it is safe e.g. to publish (personal) data on those platforms, as it would just resemble sharing information with friends as it used to be face-to-face. However, a closer look at some features in some services reveals that this parallel has some weaknesses, including that the notion of "friends" in cyberspace may in many cases substantially differ from the more traditional idea of friendship, and that a community may be very big[6]. If users are not openly informed about how their profile information is shared and what they can do to control how it is shared, they may by the notion of "community" as set out above be lured into thoughtlessly sharing their personal data they would not otherwise. The very name of some of these platforms (e.g. "MySpace") creates the illusion of intimacy on the web.

3. *"Free of charge" may in fact not be "for free"*, when users of many social network services in fact "pay" through secondary use of their personal profile data by the service providers, e.g. for (targeted) marketing.

4. *Traffic data collection by social network service providers*, who are technically capable of recording every single move a user makes on their site; eventually sharing of personal (traffic) data (including users' IP-addresses which can in some cases also resemble location data) with third parties (e.g. for advertising or even targeted advertising). Note that in many jurisdictions these data will also have to be disclosed to law enforcement and/or (national) secret services upon request, including maybe also foreign entities under existing rules on international cooperation.

5. *The growing need to refinance services and to make profits may further spur the collection, processing and use of user data*, when they are the only real asset of social network providers. Social network sites are not – while the term "social" may suggest otherwise – public utilities. At the same time, Web 2.0 as a whole is "growing up", and there is a shift from startups sometimes run by groups of students with less financial interests to major international players entering the market. This has partially changed the rules of the game, as many of these companies noted on national stock markets are under extreme pressure from their investors to create and maximise profits. As for many providers of social networks user profile data and the number of unique users (combined with frequency of use) is the only real asset these companies have, this may create additional risks for unproportional collection, processing and use of users' personal data. Note that at present, many providers of

[6] While some service providers have tried to create limited areas within their services to give users more control over how they share their (personal) information, others make such information or parts thereof available to a bigger audience, which can in some cases be the entire community – and thus millions of perfect strangers: "it stays between us", yes, but "us" may well be 50 million+.

social network services follow the concept of externalisation of privacy costs to users[7].

6. *Giving away more personal information than you think you do:* For example, photos may become universal biometric identifiers within a network and even across networks. Face recognition software has been dramatically improved over the past years, and will continue to reap even "better" results in the future. Note that once a name can be attached to a picture, this can also endanger the privacy and security of other, possibly pseudonymous or even anonymous user profiles (e.g. dating profiles, which normally have a picture and profile information, but not the real name of the data subject published). Additionally, the European Network and Information Security Agency points to an emerging technology called "content based image retrieval" (CBIR), which creates additional possibilities for locating users by matching identifying features of a location (e.g. a painting in a room, or a building depicted) to location data in a database[8]. Furthermore, "social graph" functionalities popular with many social network services do reveal data about the relationships between different users.

7. *Misuse of profile data by third parties:* This is probably the most important threat potential for personal data contained in user profiles of social network services. Depending on available privacy (default) settings and whether and how users use them, and as well on the technical security of a social network service, profile information, including pictures (which may depict the data subject, but also other people) are made available to – in the worst case – the entire user community. At the same time, very little protection exists at present against copying any kind of data from profiles, and using them for building personal profiles, and/or re-publishing them outside of the social network service[9].

   But even "normal" uses of (user) profile data uses can encroach upon users' informational self-determination and, for example, also severely limit their career prospects[10]: One example that has gained public attention is person-

[7] Cf. the statement of John Lawford from the Canadian Public Interest Advocacy Center in a speech given 3 October 2007 at the OECD-Canada Technology Foresight Forum "Confidence, privacy and security"; cf. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf [accessed 6 February 2008], p. 35

[8] Cf. ENISA Position Paper No. 1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[9] Note that some social network services allow search engines to crawl user content, and that search engine services have emerged recently specialising in offering personal profiles drawn together from different sources. On the other hand, service providers seem to have at present little or no control over the actions of spiders on their websites who do not respect the "robots.txt" protocol.

[10] "APRIL 26--A Pennsylvania woman claims that her teaching career has been derailed by college administrators who unfairly disciplined her over a MySpace photo that shows her wearing a pirate hat and drinking from a plastic cup. In a federal lawsuit, […] charges that Millersville University brass accused her of promoting underage drinking after they discovered her MySpace photo, which was captioned „Drunken Pirate". Quoted from http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [accessed 11 February 2008]. Cf. also The Guardian, January 11, 2008: "Would-be students checked on Facebook"; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html

nel managers of companies crawling user profiles of job applicants and/or employees, which seems to emerge as a steady feature: According to press reports, already today one third of human resources managers admit to use data from social network services for their work, e.g. to verify and/or complete data of job applicants[11]. Law enforcement agencies and secret services (including from less democratic countries with low privacy standards) are other entities likely to capitalise on these sources[12]. In addition, some social network service providers make available user data to third parties via application programming interfaces, which are then under control of these third parties[13].

8. *The Working Group is especially concerned about* further increased risks of identity theft fostered by the wide availability of personal data in user profiles[14], and by possible hijacking of profiles by unauthorised third parties.

9. *Use of a notoriously insecure infrastructure:* Much has been written over the (lack of) security of information systems and networks, including web services. Recent incidents include well-known service providers like Facebook[15], flickr[16], MySpace[17], Orkut[18] and the German provider "StudiVZ"[19]. While service providers have taken measures to strengthen the security of their systems, there is still room for improvement. At the same time, it is likely that new security leaks will keep emerging in the future, and is unlikely

[11] Cf. e.g. "Employers Use „Facebook" and "MySpace" to Weed Out Applicants"; http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453 [accessed 12 February 2008]. Finland seems to be the only country so far to ban such practices.

[12] Other examples to emerge in the future may well include use by immigration authorities when travelling abroad.

[13] Cf. e.g. "Facebook API Unilaterally Opts Users Into New Services", by Ryan Singel, 25 May 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; cf. also Chris Soghoian: "Exclusive: The next Facebook privacy scandal", 23 January 2008, http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [accessed 12 February 2008]

[14] Cf. as a telling example for instance the recent "Natalie"- and "frog-" experiments conducted by the Security company Sophos; cf. "Sophos Facebook ID probe shows 41 % of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites", August 2007; http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html and "Der Fall 'Natalie'. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites", 21 January 2008 (in German language) http://www.sophos.de/pressoffice/news/articles/2008/01/security-report.html

[15] Cf. "Secret Crush Facebook App Installing Adware, Security Firm Charges", Wired of 3 January 2008, http://blog.wired.com/27bstroke6/2008/01/secret-crush-fa.html

[16] Cf. "Phantom Photos: My photos have been replaced with those of another"; http://flickr.com/help/forum/33657

[17] Cf. e.g. the December 2006 "MySpace XSS QuickTime Worm"; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708

[18] Cf. PC World: "Worm Hits Google's Orkut" of 19 December 2007, http://www.pcworld.com/article/id,140653-c,worms/article.html , and SC Magazine US: "Google's Orkut hit by self-propagating trojan" of 26. February 2008, http://www.scmagazineus.com/Googles-Orkut-hit-by-self-propagating-trojan/article/107312/ [both accessed 3 March 2008]

[19] Cf. e.g. „Datenleck beim StudiVZ? [Update]"; http://www.heise.de/newsticker/meldung/81373/ (in German language)

that 100% security will ever be realised at all given the complexity of software applications at all levels of Internet services[20].

10. *Existing unsolved security problems of Internet services* add to risk of using social network services and may also in some cases raise the level of risk, or develop "flavours" specific to social network services. A recent position paper by the European Network and Information Security Agency (ENISA) inter alia lists SPAM, cross site scripting, viruses and worms, spear-phishing and social network-specific phishing, infiltration of networks, profile-squatting and reputation slander through ID theft, stalking, bullying, and corporate espionage (i.e. social engineering attacks using social network services)[21]. According to ENISA, "social network aggregators" pose an additional security threat[22].

11. *The introduction of interoperability standards and application programming interfaces* (API; e.g. "open social" introduced by Google in November 2007) to make different social network services technically interoperable entails additional new risks: They allow for automatic evaluation of all social networks websites implementing this standard. The API delivers literally the entire functionality for automatic evaluation implemented in the web interface. Possible applications with potential repercussions on user privacy (and possibly also on the privacy of non-users whose data are part of a user profile) may include: Global analysis of (professional and private) user relationships, which may well cross "borders" between different networks where user act in different roles (e.g. professionally oriented vs. more leisure-oriented networks). Interoperability may also further foster download and third-party reuse of profile information and photos, and creation of profiles about change histories of user profiles (including making available of information a user has deleted from his profile).

Guidance

Based on the above said, the Working Group makes the following (preliminary) recommendations to regulators, providers and users of social network services:

[20] In addition, the steep growth of information stored electronically every year is in itself seen as a security risk: At the last RSA Europe Security Conference in London in 2007, RSA president Art Coviello was cited saying that alone in 2006 176 exabytes of data had been generated worldwide, and that such a huge amount of data was in his view unmanageable, and could not be secured effectively; cf. the German Computer Magazine "iX", December 2007, p. 22 "Trübe Aussichten: Große Datenmengen verhindern Datensicherheit" (in German language); http://www.heise.de/kiosk/archiv/ix/2007/12/022/

[21] Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[22] Cf. ENISA Position Paper No.1 (footnote 21 supra), p. 12

Regulators

1. *Introduce the option of a right to pseudonymous use – i.e. to act in a social network service under a pseudonym*[23] *–,* where not already part of the regulatory framework.

2. *Ensure that service providers are honest and clear about what information is required for the basic service so that users can make an informed choice whether to take up the service*, and that users can refuse any secondary uses (at least through opt-out), specifically for (targeted) marketing. Note that specific problems exist with consent of minors[24].

3. *Introduction of an obligation to data breach notification for social network services.* Users will only be able to deal especially with the growing risks of identity theft if they are notified of any data breach. At the same time, such a measure would help to get a better picture of how well companies secure user data, and provide a further incentive to further optimise their security measures.

4. *Re-thinking the current regulatory framework with respect to controllership* of (specifically third party-) personal data published on social networking sites, with a view to possibly attributing more responsibility for personal data content on social networking sites to social network service providers.

5. *Improve integration of privacy issues into the educational system.* As giving away personal data online becomes part of the daily life especially of young people, privacy and tools for informational self-protection must become part of school curricula.

Providers of social network services

Providers must have a vital self-interest in preserving security and privacy of personal data of their users. A failure to make swift progress in this field may result in loss of user confidence (which is already now considerably shaken by recent security and privacy incidents), and may well result in an economic backlash comparable to the crisis that hit the digital economy in the late 1990s.

[23] "Pseudonymous use" in this context means the right to act in a social network service under a pseudonym without having to reveal one's "true" identity to other users of the service, or to the general public, if the user wishes so. Depending on circumstances, this may well include having to reveal one's true identity vis-à-vis the provider of the social network when registering.

[24] Cf. Working Paper "Children's' Privacy On Line: The Role of Parental Consent", adopted at the 31st meeting, Auckland (New Zealand), 26/27 March 2002; http://www.datenschutz-berlin.de/attachments/205/child_en.pdf?1200656702

1. *Transparent and open information of users* is one of the most important elements of any fair processing and use of personal information. While the need for such a mechanism is recognised in most national, regional and international regulatory instruments for privacy, the present form in which many service providers inform their users may need to be revisited: At present – and in many cases in line with existing regulatory frameworks – privacy information form a part of sometimes complex and lengthy "terms and conditions" of a service provider. In addition, a privacy policy may be provided. Some service providers suggest that the percentage of users actually downloading this information is very low[25]. Even if this information is displayed on the screen when a user signs up to a service, and can also be accessed later if the user so wishes, the goal to inform users about potential consequences of their actions during the use of a service (e.g. when changing privacy settings for a collection of – say – pictures) may be better served by built-in, context-sensitive features, that would deliver the appropriate information based on user actions.

   User information should specifically comprise information about the jurisdiction under which the service provider operates, about users' rights (e.g. to access, correction and deletion) with respect to their own personal data, and the business model applied for financing the service. Information must be tailored to the specific needs of the targeted audience (especially for minors) to allow them to make informed decisions.

   Information of users should also refer to third party data: Providers of social network services should – on top of informing their users about the way they treat their (the users') personal data, also inform them about the do's and don'ts of how they (the users) may handle third party information contained in their profiles (e.g. when to obtain the data subjects' consent before publication, and about possible consequences of breaking the rules). Especially the huge quantities of photos in user profiles showing other people (in many cases even tagged with name and/or link to the other persons' user profile) are an issue in this context, as current practices are in many cases not in line with existing legal frameworks governing the right to control one's own image.

   Candid information should also be given about remaining security risks, and possible consequences of publishing personal data in a profile, as well as about possible legal access by third parties (including also e.g. law enforcement, secret services).

2. *Introduce the creation and use of pseudonymous profiles as an option*, and encourage its use.

[25] A representative from facebook stated recently at an OECD conference that the percentage of users visiting a privacy policy may not be more than a **quarter of a percent**; cf. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf p. 33f. [accessed 6 February 2008].

3. *Living up to promises made to users:* A *conditio sine qua non* for fostering and maintaining user trust is clear and unambiguous information about how their information will be treated by the service provider, specifically when it comes to sharing personal data with third parties. However, with some service providers there are at present ambiguities with respect to those promises. The most prominent example is the popular statement "we will never share your personal information with third parties" in relation to targeted advertising. While this statement may be formally correct in the eyes of the service provider, some providers fail to clearly communicate the fact that e.g. for displaying advertisements in the browser window of a user, the IP address of these users may be transmitted to another service provider delivering the content of the advertisement, in some cases based on information processed by the social network service provider from a users' profile. While the profile information itself may indeed not be transmitted to the advertisement provider, the users' IP address will[26] (if the social network provider does not e.g. use a proxy mechanism to hide the user IP address from the provider of the advertisement). The problem is that some providers of social network services erroneously assume that IP addresses are not personal data, while in most jurisdictions they in fact often are. Such ambiguities may mislead users and may spur an erosion of trust when users learn about what happens in reality, which is neither in the interest of the users, nor in the interest of the service provider. Similar problems exist regarding the use of cookies.

4. *Privacy-friendly default settings* play a key role in protecting user privacy: It is known that only a minority of users signing up to a service will make any changes to default settings – including privacy settings. The challenge for service providers here is to choose settings that offer high degree of privacy by default without making the service unusable. At the same time, usability of setting features is key to encourage users to make their own changes. In any case, non-indexibility of profiles by search engines should be a default.

5. *Improve user control over use of profile data:*

   - *within the community*; e.g. allow restriction of visibility of entire profiles, and of data contained in profiles, as well as restriction of visibility in community search functions. Tagging of photos (i.e. the addition of links to an existing user profile or the naming of depicted persons) should be bound to the data subject's prior consent.

   - *create means allowing for user control over third party use of profile data* – vital to especially address risks of ID theft. However, there are at

[26] Depending on circumstances, the advertisement provider may even be able to reconstruct some or all of the underlying profile information based on the kind of targeted advertisement that is to be displayed to a specific user.

present only limited means to control information once it is published. The experience of the movie and music industries with digital rights management technologies suggests that possibilities may in this respect stay limited. Nevertheless, services providers should strengthen research activities in this domain: Existing and maybe promising approaches include research on the "semantic" or "policy-aware web[27]", encrypting user profiles, decentralise storage of user profiles (e.g. with users themselves), the use of watermarking technologies for photos, the use of graphics instead of text for displaying information, and the introduction of an expiration date to be set by users for their own profile data[28]. Service providers should also strive to discourage secondary use especially of pictures by offering a function allowing users to pseudonymise or even anonymise pictures[29]. They should also take effective measures to prevent spidering, bulk downloads (or bulk harvesting) of profile data. Specifically, user data should only crawled by (external) search engines if a user has given his explicit, prior and informed consent.

- *Allow for user control over secondary use of profile and traffic data;* e.g. for marketing purposes, as a minimum: opt-out for general profile data, opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data. Many existing legal frameworks contain binding rules on secondary uses for marketing purposes, which must be observed by providers of social network services. Consider letting users decide for themselves, which of their profile data (if any) they would like to be used for targeted marketing. In addition, the introduction of a fee should be considered as an additional option at the choice of the user for financing the service instead of use of profile data for marketing.

- *Comply with user rights recognised in national, regional and international privacy frameworks;* including the right of data subjects to have data – which may well be entire profiles – erased in a timely manner.

- *Address the issues that may arise in cases of a takeover or merger of a social network service company:* Introduce guarantees for users that new owner will maintain present privacy (and security) standard.

---

[27] Cf. e.g. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: "Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web". To appear in: Web and Information Security, E. Ferrari and B. Thuraisingham (eds), Idea Group Inc., Hershey, PA (forthcoming); http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf , and Sören Preibusch, Bettina Hoser, Seda Gürses, and Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [both accessed 12 February 2008].

[28] Cf. e.g. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. March 2007, at 7.2.1, p. 40

[29] Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, p.23

6. *Appropriate complaint handling mechanisms* should be introduced (e.g. to "freeze" contested information, or pictures), where they do not already exist, for users of social networks, but also with respect to third party personal data. Timely response to data subjects is important. Measures may also include a penalty mechanism for abusive behaviour with respect to profile data of other users and third party personal data (incl. removing users from site as appropriate).

7. *Improve and maintain security of information systems.* Use recognised best practices in planning, developing, and running social network service applications, including independent certification.

8. *Devise and/or further improve measures against illegal activities, such as spamming, and ID theft.*

9. *Offer encrypted connections for maintaining user profiles,* including secured log-in.

10. Social network providers acting in different countries or even globally should respect the privacy standards of the countries where they operate their services.

Users of social networks

1. *Be careful.* Think twice before publishing personal data (specifically name, address, or telephone number) in a social network profile. Think also about whether you would like to be confronted with information or pictures in a job application situation. Maintain your profile information. Learn from CEOs of big companies: These people know about the value of their personal information and control it. This is why you will not find a lot of personal information about them on the web.

2. *Think twice before using your real name in a profile.* Use a pseudonym instead. Note that even then you have only limited control over who can identify you, as third parties may be able to lift a pseudonym, especially based on pictures. Think of using different pseudonyms on different platforms.

3. *Respect the privacy of others.* Be especially careful with publishing personal information about others (including pictures or even tagged pictures), without that other person's consent. Note that illegal publication especially of pictures is a crime in many jurisdictions.

4. *Be informed:* Who operates the service? Under which jurisdiction? Is there an adequate regulatory framework for protecting privacy? Is there an independent oversight mechanism (like a Privacy Commissioner) that you can turn to in case of problems? Which guarantees does the service provider give with respect to handling your personal data? Has the service been certified by independent and trustworthy entities for good quality of privacy, and security? Use the web to educate yourself about other people's experience with the privacy and security practices of a service provider you do not know. Use existing information material from providers of social network services, but also from independent sources like Data Protection Agencies[30], and security companies[31].

5. *Use privacy friendly settings.* Restrict availability of information as much as possible, especially with respect to indexing by search engines.

6. *Use different identification data* (e.g. login and password) than those you use on other websites you visit (e.g. for your e-mail or bank account).

7. *Use opportunities to control* how a service provider uses your personal (profile and traffic) data. E.g. opt out of use for targeted marketing.

8. Pay attention to the activity of your children in the Internet, especially on social network websites.

Closing remark

The Working Party calls upon Consumer and Privacy Protection Organisations to take appropriate measures to raise awareness with regulators, service providers, the general public, and notably young people[32] about privacy risks regarding the use of social networks and responsible behaviour with respect to one' own personal data, as well as those of others.

The Working Group will closely monitor future developments with respect to the protection of privacy in social network services and revise and update this Guidance as necessary.

---

[30] Cf. e.g. the brochure "when online gets out of line" jointly published by facebook and the Information and Privacy Commissioner of Ontario, Canada, at http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf, the US Federal Trade Commission: "Social Networking Sites: A Parent's Guide" at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm and "Social Networking Sites: Safety Tips for Tweens and Teens" at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

[31] Cf. e.g. the model privacy settings proposed by Sophos for facebook; http://www.sophos.com/security/best-practice/facebook.html

[32] Cf. e.g. the campaign „dubestemmer" launched by the Norwegian Data Protection Authority; http://www.dubestemmer.no/english.php, the "DADUS"-Project of the Portuguese Data Protection Authority; http://dadus.cnpd.pt, and the initiatives cited in footnote 30 above

2009

45. Sitzung, 12. und 13. März 2009, Sofia, Bulgarien

Bericht und Empfehlungen zu Mautsystemen

– „Sofia Memorandum“ –

Empfehlungen:

Die Arbeitsgruppe empfiehlt, dass die Hersteller von großangelegten Mautsystemen, die persönliche Daten verarbeiten, die folgenden Empfehlungen zum Schutz der Privatsphäre der Fahrer und der Fahrzeugeigentümer einhalten:

- Die Anonymität der Fahrer kann und sollte durch die Verwendung der sogenannten „Smart-Clients“ oder anonymen Proxies gewahrt werden, die die persönlichen Daten der Fahrer unter deren alleiniger Kontrolle halten und keine Speicherung der Daten außerhalb des Fahrzeugs erfordern.

- Mautsysteme können und sollten so entworfen werden, dass die detaillierten Routendaten gänzlich und dauerhaft aus dem System gelöscht werden, nachdem die Gebühren festgesetzt wurden, um zu vermeiden, dass Bewegungsprofile erstellt oder die Daten zweckentfremdet werden.

- Die Verarbeitung von persönlichen Daten zu anderen Zwecken (z. B. „pay-as-you-drive“-Versicherungen oder verhaltensbasierte Werbung) sollte nur mit der eindeutigen und ausdrücklichen Einwilligung des Betroffenen möglich sein.

- Im Hinblick auf die Durchsetzung sollte das System die Identität der Fahrer oder Fahrzeugbesitzer nicht feststellen, solange nicht der Verdacht besteht, dass der Fahrer eine Zuwiderhandlung begangen hat, die als Verstoß gegen das Mautsystem definiert wird.

Hintergrund:

Großangelegte Mautsysteme, die auf einer „pay as you go“-Basis im fließenden Verkehr angelegt sind, sind keine neue Erfindung. Überlegungen zu elektronischen Mautsystemen kamen in den letzten Jahrzehnten des 20. Jahrhunderts auf[1]. Verschiedene Begriffe werden verwendet, um die Nutzung moderner Infor-

[1] Electronic Road Charging: http://www.parliament.uk/post/pn112.pdf.

mations- und Kommunikationstechnologien für Mautsysteme zu beschreiben; dazu gehören „elektronische Verkehrsgebühr", „Intelligente Verkehrssysteme" (IVS), „elektronische Mauterhebung", „Straßennutzungsgebühr", „Zeit-, Entfernungs-, Ortsgebühren", „entfernungsbasierte Straßennutzungsgebühr", „vehicles miles travelled (VMT) charging" und verschiedene weitere.

Bestehende Mautsysteme können Gebühren auf Autobahnen erheben oder eine Abgabe verlangen, wenn eine bestimmte Zone mit dem Fahrzeug befahren wird. Sie sind jedoch nicht in der Lage, Gebühren mittels eines Algorithmus zu errechnen, der an „Zeit, Strecke und Ort" gebunden ist, was für großangelegte Anwendungen erforderlich wäre. Das erwünschte Resultat eines elektronischen Mautsystems ist die Möglichkeit, nach der *tatsächlichen* Nutzung abrechnen zu können (z. B. je mehr man fährt, desto mehr zahlt man), in Abhängigkeit von der Uhrzeit der Fahrt (z. B. weniger in Zeiten außerhalb des Berufsverkehrs) und in einem variierenden Tarif, der sich anhand der gewählten Straße ermitteln lässt. Der Verkehrsfluss könnte in diesen Systemen dadurch verbessert werden, dass die Fahrer nicht gezwungen wären, an bestimmten Abrechnungsstellen anzuhalten. Prinzipiell wäre dies die gerechteste und ökologisch wünschenswerteste Möglichkeit zu bezahlen – so wie Verbraucher gewöhnlich für ihren Wasser- oder Stromverbrauch zahlen.

Abgesehen von Mautgebühren gibt es zahlreiche andere Dienste, die auf Daten in Bezug auf Zeit, Ort und zurückgelegte Strecke basieren, wie zum Beispiel Parksysteme, „pay-as-you-drive"-Versicherungen, Parkplatzfinder oder -versteigerer, die Rationierung von Straßenraum, Parkplatz-Treue-Programme, Staumelde- und Gebührensysteme, Routenplaner („Sie könnten 12 € pro Woche sparen, wenn Sie jeden Tag 30 Minuten früher losfahren würden") und intelligente Transportsysteme („Wenn Sie heute die A 2 nutzen statt der A 3, sparen Sie 20 %"). Während die elektronische Erhebung und Verarbeitung von Daten in Bezug auf den Ort, die Identifikation einer Person sowie die Reisedaten schon heute für verschiedene Zwecke genutzt werden kann und somit auch mehrere sozioökonomische Probleme hervorruft, bezieht sich dieses Dokument vornehmlich auf datenschutzrechtlich relevante Auswirkungen von (großangelegten) elektronischen Mautsystemen.

Um besser nachvollziehen zu können, worin die datenschutzrechtlichen Auswirkungen bestehen, müssen einige der Grundprinzipien dieser Systeme näher betrachtet werden. Großangelegte Maut-Initiativen, die die Verarbeitung persönlicher Daten implizieren (andere als z. B. bei Vignetten, anonymen Aufklebern und Signalen sowie Gebührensysteme mit Mautstationen, die keinen freien Verkehrsfluss ermöglichen) werden weltweit entwickelt, z. B. in den USA (Oregon und der Puget Sound Region), Australien, Neuseeland, Kanada (auf der Schnellstraße 407), das Toll Collect System in Deutschland[2] und die in den Niederlan-

[2] Es muss darauf hingewiesen werden, dass das deutsche System nur für Lastkraftwagen gilt: http://www.toll-collect.de.

den[3] und Norwegen bestehenden Mautpläne. In der EG wird darüber hinaus mit der Richtlinie 2004/52/EG das Ziel verfolgt, das „pay as you go"-Prinzip im freien Verkehrsfluss in den zukünftigen Europäischen Elektronischen Mautdienst (European Electronic Toll Service – EETS) einfließen zu lassen. In seiner letzten Stufe der Entwicklung soll dieses europaübergreifende System die Möglichkeit bieten, Verkehrsgebühren für alle Arten von Straßen einschließlich Viadukten, Tunneln und anderen Objekten zu erheben. Mit dem neuen Abrechnungssystem sollen Fahrer die Gebühren zahlen können, ohne anhalten zu müssen und dadurch Verkehrsstauungen zu verursachen. Gleichzeitig ermöglicht es diese Einrichtung auch, Gebühren für alle kostenpflichtigen Autobahnen in Europa zu erheben.

Der Grund, warum die Debatten über Straßennutzungsgebühren so emotional aufgeladen sind, liegt darin, dass ortsbezogene Daten, Daten zur Identifikation und Abrechnungsdaten zusammengeführt werden. Mit anderen Worten, es wird bekannt, wer zu welcher Zeit wo war, um dafür Gebühren abzurechnen. Um das „pay as you go"-Prinzip im freien Verkehrsfluss umzusetzen (und um über ein interoperatives System zu verfügen), können Mautsysteme eine massive Überwachung der Bewegung von Personen (Fahrzeuginhaber und Fahrer) mit sich bringen. Daher müssen die Auswirkungen auf die Privatsphäre der Betroffenen sorgfältig untersucht werden. Es ist nicht schwierig, sich den enormen Wert einer zentralisierten Datenbank über das Bewegungsverhalten von Fahrern und zahlreiche Szenarios für eine Zweckentfremdung der Daten vorzustellen, bei denen Daten für andere Zwecke genutzt werden als die für die sie ursprünglich erhoben wurden (z. B. Mautgebühren). Zahlreiche Datenschutzbeauftragte haben bereits Stellungnahmen und Empfehlungen zum Schutz der Privatsphäre im Zusammenhang mit Mautsystemen erstellt (z. B. Ontario[4], Niederlande[5], Victoria/Australien[6], Norwegen[7] und Slowenien[8]). Fehlwahrnehmungen hinsichtlich der Auswirkungen auf die Privatsphäre werden tatsächlich häufig als eines der größten Hindernisse für die Einführung großangelegter Mautsysteme betrachtet.

Grundsätzlich werden zwei etablierte Technologien für diese Systeme in Erwägung gezogen: short range communications (DSRC[9], das auch als „tag-beacon-

[3] Ministerium für Verkehr, Öffentliche Arbeit und Wassermanagement: Implementierung des Maut-Systems: http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/roadpricing/index.aspx

[4] 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner Ontario: http://www.ipc.on.ca/images/Resources/407-e.pdf.

[5] http://www.curacaoproject.eu/documents/newsletter-issue3.pdf.

[6] Eine ausführliche Studie von Mautsystemen und eine vollständige Liste an Quellen wurde durch Victoria Transport Policy Institut vorbereitet: Road Pricing, Congestion Pricing, Value Pricing, Toll Roads and HOT Lanes; http://www.vtpi.org/tdm/tdm35.htm.

[7] Road Reform and Privacy: Which Way Forward? Submission by the Privacy Commissioner to the Ministry of Transport in relation to the final report of the Roading Advisory Group: http://www.privacy.org.nz/road-reformand-privacy-which-way-forward/?highlight=impact.

[8] http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=568.

[9] DSRC - Dedicated Short Range Communications.

System“ bezeichnet wird) und globale Satellitennavigationssysteme (GNSS/SN[10]), welche die Position des Fahrzeugs bestimmen und die Daten über leistungsstarke drahtlose Kommunikationsnetzwerke übertragen, wobei das letztgenannte oftmals als satellitengestütztes Mautsystem bezeichnet wird.

Jedes dieser Systeme hat seine Vor- und Nachteile: die DSRC-basierten technischen Lösungen sind z. B. weiter verbreitet und wurden häufiger getestet, aber sie sind nicht auf allen Straßen anwendbar.[11] Die Wahl der Technologie hängt hauptsächlich von der Größe der Implementierung ab und unterscheidet sich in der Umsetzung nach relativ kleinen Gebieten (z. B. Großstädte[12]) und großen Gebieten (z. B. landesweit oder sogar international). Im Hinblick auf großangelegte Implementierungen scheint die DSRC-basierte Technologie an Boden zu verlieren. Wegen der enormen Anzahl an abzudeckenden Straßen sind Lösungen, die beträchtliche Infrastrukturen am Straßenrand erfordern, wie bestehende DSRC-basierte Umsetzungen, nicht so sehr geeignet, wenn auf allen Straßen Gebühren erhoben werden sollen.[13] Diese Sichtweise wird auch in einem neuen Bericht der National Surface Transportation Infrastructure Financing Commission der USA wiedergegeben.[14] Der Vorteil eines Satellitensystems besteht in seiner Flexibilität, wobei solche Systeme auf der anderen Seite noch nicht umfassend in der Praxis getestet wurden.

Die Verwendung elektronischer Mautsysteme ist, – die vielen sozio-ökonomischen Debatten und Probleme außer Acht lassend – oftmals durch zwei gebräuchliche datenschutzrechtliche Fehleinschätzungen gehemmt, die von der allgemeinen Öffentlichkeit und der Presse vertreten werden und denen entschieden entgegengetreten werden muss.

Erstens betont die Arbeitsgruppe, es muss keine Befürchtungen der Art geben, dass GPS-basierte Ansätze bedeuten würden, dass eine allumfassende Datenbank über die Position von Fahrzeugen in einer „Big Brother im Himmel“-Manier aufgebaut würde. Das GPS der USA, das russische GLONASS sowie das zukünftige Satellitensystem Galileo basieren auf passiven Empfängern, die unter Verwendung von Satelliteninformationen den Aufenthaltsort des Fahrzeugs berechnen; diese Empfänger können die Information über den Aufenthaltsort des Fahrzeugs nicht zurück zum Satelliten übermitteln. Daher müssen wir verstehen, wenn die Entscheidung für ein Satellitensystem fallen soll, dass durch Satellitennavigation

[10] GNSS/CN - Global Navigation Satellite System/Cellular Networks.

[11] Privacy-Sensitive Congestion Charging. Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle: http://www.cl.cam.ac.uk/~arb33/papers/BeresfordDaviesHarle-PrivacyAwareCongestion-SPW2006.pdf.

[12] Singapore, Melbourne, Trondheim, Toronto sind Beispiele für Systeme in Großstädten.

[13] Stefan Eisses, Wiebren de Jonge und Vincent Habers: Privacy And Distance Based Charging For All Vehicles On All Roads.Sh: http://www.tipsystems.nl/files/Privacy_and_RUC_ITSLondon-doc.pdf.

[14] National Surface Transportation Infrastructure Financing Commission: Paying Our Way, a New Framework for Transportation Finance, February 24, 2009 http://www.itif.org/index.php?id=227.

ein Fahrzeug lediglich die Information über seine Position erhält, während die Ortsangaben an die Kontrollstelle des Mautabrechnungssystems über drahtlose Netzwerke übermittelt werden, so z. B. durch das GSM-Netz. Eine allumfassende Datenbank mit ortsbezogenen Daten und Identifikationsdaten könnte daher nur „vor Ort" in den Kontrollstellen entstehen: Genau davon handelt dieses Dokument.

Zweitens wird häufig der Vergleich zu Mobiltelefonen oder zu Kreditkarten gezogen, wo persönliche Daten nachverfolgt werden oder nachverfolgt werden können. Die Arbeitsgruppe möchte hervorheben, dass vereinfachende Vergleiche dieser Art nicht angemessen sind, vor allem weil Gebührenerfassungsgeräte ununterbrochen in Betrieb sein müssen (zumindest auf kostenpflichtigen Straßen), anders als im Fall von Mobiltelefonen, deren Benutzung völlig freiwillig ist. Die Möglichkeit, das Gerät auf kostenpflichtigen Straßen abzuschalten, würde es einfacher machen, die Gebührenerfassung zu umgehen, und aus diesem Grund werden die Auswirkungen von Mautsystemen auf die Privatsphäre sogar noch relevanter.

Die Verteilung des Abrechnungsprozesses

Der Abrechnungsprozess ist in vier Phasen unterteilt:

1. Bestimmung der Position des Fahrzeugs,
2. Bestimmung des Abschnitts der Straße oder Gebührenelements und des dazugehörigen Tarifs,
3. Berechnung des Betrags, der für diesen Bereich fällig wird,
4. Berechnung des Gesamtbetrages, der für die ganze Fahrt fällig wird.

Ein entscheidender Faktor, wenn man die datenschutzrechtlichen Auswirkungen bestimmen möchte, ist, wie die Phasen des Abrechnungsprozesses zwischen den verschiedenen datenverarbeitenden Stellen verteilt werden. Die vier Phasen des Abrechnungsprozesses können entweder von einer Stelle vorgenommen oder zwischen zwei oder mehreren aufgeteilt werden. Konsequenterweise unterscheiden sich die datenschutzrechtlichen Auswirkungen der verschiedenen Ausführungsmodelle. Einige der Modelle werden im Folgenden vorgestellt, zusammen mit den wichtigsten Kriterien, die beachtet werden müssen, wenn man die datenschutzrechtlichen Auswirkungen ermitteln möchte. Die zwei Hauptmodelle für Mautsysteme werden als **Thin-Client-Ansatz** und **Smart-Client-Ansatz** bezeichnet; allerdings gibt es zwischen diesen beiden Systemen noch andere Modelle, so wie der sogenannte Distributed-Role-Ansatz und Proxies. Diese vier Ansätze werden im Folgenden diskutiert.

Der „Thin-Client"-Ansatz

Die im Hinblick auf den Schutz der Privatsphäre am wenigsten favorisierte Variante eines Mautsystems liegt vor, wenn alle Daten über die Reisezeit und die Position der Fahrzeuge an eine einzige Stelle oder Institution, die als Kontrollzentrum agiert, gesendet und dort gespeichert werden. Der sogenannte „Thin-Client" (oder „On-Board-Unit" - OBU) sammelt nur Daten über zurückgelegte Strecken; alle vier Phasen des Abrechnungsprozesses werden durch die Kontrollstelle unter Verwendung einer zentralen Datenbank mit ortsbezogenen Daten, Identifikationsdaten und Abrechnungsdaten verarbeitet.

Die Arbeitsgruppe äußert ihre Bedenken hinsichtlich der Übernahme dieses Ansatzes, denn er bietet offensichtlich den geringsten Schutz für die Privatsphäre der Betroffenen. Im Prinzip ist die Frage, ob man „Thin-Clients" oder „Smart-Clients" bevorzugt, eine Frage von zentralisierter gegenüber dezentralisierter Datenverarbeitung, ein Dilemma, dem der Schutz der Privatsphäre und der Datenschutz oft begegnet.

Die Befürworter einer zentralisierten Datenbank behaupten, wenn die Daten geschützt durch angemessene Maßnahmen zur Datensicherung (z. B. entsprechende Zugangskontrolle, Protokollierung der Verarbeitung persönlicher Daten usw.) zentral gespeichert werden, könne ein höheres Sicherheitslevel gewährleistet werden, als es eine Einzelperson tun könne. Ein Gegenargument ist allerdings, dass dort, wo die Daten unter der Kontrolle eines Einzelnen sind, nur dessen Daten gefährdet sind (z. B. wenn das Fahrzeug oder das im Fahrzeug installierte Gebührenerfassungsgerät gestohlen wurden), wohingegen in dem zentralisierten Verarbeitungssystem persönliche Daten potentiell aller Betroffenen gefährdet sind (trotz eines möglicherweise höheren Grades an Sicherheit). Aus diesem Grund sind aus der Perspektive des Schutzes der Privatsphäre Lösungen zu befürworten, wo persönliche Daten nicht zentralisiert gespeichert werden, sondern im Besitz und unter der Kontrolle des Nutzers bleiben. Darüber hinaus begegnen Datenschützer regelmäßig dem Problem der zweckfremden Nutzung (dem sog. „function creep"-Phänomen) – dabei werden Daten, die ursprünglich für einen bestimmten Zweck erhoben wurden (der völlig legitim und gesetzeskonform sein kann), später für einen völlig anderen Zweck genutzt, ein Zugriff auf die Daten ist vorher unvorhergesehenen Dritten möglich, usw.

Der „Distributed-Role"-Ansatz

Manche Modelle schlagen den sogenannten Distributed-Role-Ansatz vor, der vermutlich einen besseren Schutz der Privatsphäre und der persönlichen Daten bietet. Der Distributed-Role-Ansatz stellt eine Lösung dar, die auf dem Prinzip basiert, die Daten zwischen zwei Stellen oder Parteien zu verteilen, wobei eine

Partei die ortsbezogenen Daten und die Abrechnungsdaten hat und die andere nur die Identifikationsdaten der Fahrer.

Die erste Stelle oder Partei verfügt über die Identifikationsnummer des Geräts, das sich im Fahrzeug befindet, und empfängt Informationen über die Strecke, die das Fahrzeug zurücklegt (Fahrtdauer und Position), weiß aber nicht, wer der Inhaber des Geräts ist. Basierend auf diesen Informationen berechnet diese Partei die fälligen Gebühren. Die Ergebnisse dieser aggregierten Berechnungen (nur die Gebührensumme in einer bestimmten Periode, ohne Informationen über Fahrtzeit und Position) werden zusammen mit der Identifikationsnummer des Geräts an eine andere Partei übermittelt, die den Besitzer des Gerätes identifizieren kann, von dem dann die Gebühr erhoben wird; jedoch sammelt diese zweite Partei keine Informationen über die Reise des Fahrzeugs. Die Befürworter dieses Ansatzes berufen sich häufig darauf, dass durch die Verteilung der Rollen insgesamt keine Verarbeitung personenbezogener Daten stattfindet. Die Arbeitsgruppe stellt eine solche Begründung allerdings in Frage, denn eine große Menge an personenbezogenen Daten wird immer noch von den verschiedenen Parteien verarbeitet.

Diese Lösung schützt die Privatsphäre eines Betroffenen nur scheinbar, auch wenn eine Partei nur die Information über die Position des Fahrzeuges und die Reisedauer sammelt und die Identität des Fahrers nicht kennt und umgekehrt. Innerhalb dieses Ansatzes werden immer noch von einer Stelle große Mengen an Daten gesammelt und verarbeitet; nur die Identifikationsdaten werden einer anderen Stelle oder Partei anvertraut. Die Arbeitsgruppe verweist auf die Stellungnahme der Artikel 29-Datenschutzgruppe, wonach Daten, die auf eine identifizierte oder identifizierbare natürliche Person beziehbar sind, wie personenbezogene Daten behandelt werden müssen und dass die Identifizierbarkeit eines Betroffenen nicht nur durch die Mittel und Ressourcen einer datenverarbeitenden Stelle (in diesem Fall die erste Partei) zu bestimmen ist, sondern in einem generelleren Sinn. Die datenverarbeitende Stelle sollte voraussehen, dass „die Mittel, die wahrscheinlich und vernünftigerweise genutzt werden“, um eine Person zu identifizieren, verfügbar sein werden, wie z. B. durch die angerufenen Gerichte (anders würde das Erheben der Daten keinen Sinn machen) und daher sollten diese Information als personenbezogene Daten behandelt werden. Unabhängig davon, ob die erste Partei einen Betroffenen, auf den sich die Orts- und Zeitangaben beziehen, selbst zu identifizieren vermag oder nicht, verarbeitet diese Partei unzweifelhaft personenbezogene Daten. Um dies zu untermauern: Es ist offensichtlich, dass in Fällen, in denen die Straßennutzungsgebühr nicht gezahlt wurde oder die Person sich geweigert hat, die Gebühr zu zahlen, der Gläubiger einen schnellen und einfachen Weg finden muss, die Kalkulation der Gebühr zu reproduzieren, was es erforderlich macht, die Daten über die Fahrtzeit und Position einer identifizierbaren Person zu verarbeiten. Darüber hinaus ist eine Zweckentfremdung („function creep“) der Daten erneut sehr wahrscheinlich, denn große Mengen von Daten werden zentral gespeichert.

Der „Smart-Client"-Ansatz

Um den Schutz der Privatsphäre der Betroffenen sicherzustellen, wäre sicherlich ein System am meisten geeignet, in dem die Daten, die zum Zweck der Mauterhebung erforderlich sind, ausschließlich unter der Kontrolle der Nutzer stehen. In diesem Fall würde die Berechnung der Gebühr durch das Gerät (das sogenannte intelligent device) erfolgen, wobei die Kontrollstelle nur die Summe der anfallenden Gebühren empfangen würde. Dies bedeutet, dass alle vier Abrechnungsphasen innerhalb dieses Gerätes erfolgen würden: Bestimmung der Position des Fahrzeugs; Bestimmung des Abschnitts der Straße oder Gebührenelements und des dazugehörigen Tarifs; Berechnung des Betrags, der für diesen Bereich fällig wird und Berechnung des Gesamtbetrages, der für die ganze Fahrt fällig wird.

Die Anonymität des Fahrers würde auf diesem Weg gewahrt, weil alle Daten über Position und Fahrtzeit unter der alleinigen Kontrolle des Nutzers stünden. Die Nutzer sollten sich nur selbst identifizieren, wenn gewisse Unregelmäßigkeiten auftreten, die eine Identifizierung erforderlich machen: z. B. wenn der Nutzer eine richtig berechnete Mautgebühr nicht gezahlt hat, das Fahrzeug gestohlen wurde oder wenn das Gebührenerfassungssystem des Nutzers kaputt ist oder nicht richtig funktioniert (während des Befahrens einer kostenpflichtigen Straße). Die Kontrollstelle muss nur Gewissheit darüber haben, dass das Gerät im Fahrzeug, das die Gebühren berechnet, auf kostenpflichtigen Straßen richtig arbeitet.

In einem solchen System hat die Kontrollstelle keine Daten über die Position des Fahrzeugs; sie kontrolliert nur, ob das Gerät richtig funktioniert. Dieses System erfordert natürlich einige operative Maßnahmen, wie den Schutz der Einrichtungen vor Betrug (dies umfasst die Blockierung, Verfälschung, Abschirmung, Modifikation, absichtliches Herbeiführen einer Fehlfunktion etc.). Ein sehr wichtiger Aspekt sowohl des Thin- als auch des Smart-Clients ist, dass sie nicht durch den Benutzer abgeschaltet werden können, sofern sich das Fahrzeug auf einer kostenpflichtigen Straße befindet, denn das wäre eine Umgehung der Zahlungspflicht. Der Smart-Client-Ansatz ist nicht ohne Herausforderungen, es ist zum Beispiel notwendig, passende Zertifizierungsstandards anzubieten, eine richtige Installation und die Wartung der Geräte zu gewährleisten und außerdem einige andere technische Aspekte zu beachten (z. B. Energieversorgung, Funktionskontrolle, Speicherkapazitäten) und – wahrscheinlich der wichtigste Aspekt – die Kosten.

Während der Smart-Client-Ansatz kostenintensiver erscheint als der sogenannte Thin-Client-Ansatz, hat der Smart-Client-Ansatz auch gewisse ökonomische Vorteile: Das „intelligente" Gerät ist nicht anfällig für Kommunikationsstörungen (z. B. in Regionen, in denen kein GSM-Signal verfügbar ist) oder wenn die Kontrollstelle temporär nicht betriebsbereit ist, weil der Smart-Client die Gebühr selbst errechnen kann. Auf der anderen Seite kann das Gerät, das permanent Da-

ten an die Kontrollstelle sendet und von der Kalkulation der Kontrollstelle abhängig ist (der Thin-Client) in Gebieten, in denen keine GSM-Abdeckung vorliegt oder wenn die Kontrollstelle nicht arbeitet, die Gebühr nicht allein errechnen. Es ist auch hervorzuheben, dass das „intelligente" Gerät auch Operationen im Thin-Client-Modus unterstützen kann (metaphorisch gesprochen kann der „dumme" Client nicht „intelligent" werden, während das Umgekehrte möglich ist), was eine bedeutende Voraussetzung für die Interoperabilität der Systeme ist (z. B. innerhalb des zukünftigen europäischen elektronischen Mautservices) oder mit anderen zuvor bestehenden städtischen Gebührensystemen oder City-Maut Systemen. Die Geräte in den Fahrzeugen müssen wissen, wie sie auf unterschiedliche Systeme reagieren sollen: Nachdem die Zone eines anderen Betreibers erreicht wurde, wird das Gerät Anweisungen erhalten, wie es zu arbeiten hat. Internationale Standardisierungsorganisationen (ISO und CEN) entwickeln passende technische Standards, während die Industrie bereits funktionierende Lösungen getestet hat. Während ökonomische Faktoren für die Einführung eines bestimmten Systems entscheidend sind, beeinflussen sie die datenschutzrechtlichen Implikationen nicht. Der vermeintliche Nachteil für einen Smart-Client könnte durch Massenproduktionen oder Anreize (z. B. durch die Kombination eines Freisprechmobiltelefons oder eines Satellitennavigationssystems mit dem Gerät) minimiert werden.

Der Smart-Client könnte auch eine anonyme Nutzung erleichtern, wenn Pre-Paid-Lösungen wie beim Mobiltelefon angeboten würden. Ein Fahrer sollte die Möglichkeit haben, ein Gebührenguthaben zu kaufen, das mit der On-Board-Einheit verwendet werden könnte, die dann die Kontrollstelle informieren könnte, dass die Gebühren für den Straßenabschnitt bereits vorab gezahlt wurden.

Proxies

Es sind auch weitere gemischte Ansätze bekannt und schon jetzt auf dem Markt erhältlich. Die Abrechnungsstelle kann zum Beispiel ausschließlich als technisches Zentrum agieren, als eine Art Zwischenstelle oder Proxy, der ausgewählt wird, um Berechnungen vorzunehmen. Diese Proxies (gewöhnlich als anonyme weiterleitende Proxies oder anonyme „loop-back"-Proxies bezeichnet) können im Fahrzeug oder außerhalb installiert werden und die Funktion haben, die Daten an Bord des Fahrzeugs oder an einer anderen Stelle zu speichern. Die datenschutzrechtlichen Auswirkungen eines solchen Ansatzes zu bewerten ist im Prinzip eine Frage des Vertrauens (z. B. ob dem Gerät vertraut werden kann und ob Dritte wirklich nicht in der Lage sind, auf die Daten zuzugreifen).

Die Arbeitsgruppe befürwortet generell solche Proxy-Ansätze, sofern deren Schutz der Privatsphäre unabhängig überprüft werden kann und sie den Grad an Schutz der Privatsphäre garantieren, der bei einem reinen Smart-Client-Ansatz erreicht wird.

Durchsetzung

Die Durchsetzung ist ein anderes entscheidendes Element, das in einer datenschutzfreundlichen Art und Weise gestaltet werden muss, wenn man anstrebt, die Anonymität der Fahrer in elektronischen pay-as-you-go-Mautsystemen zu wahren.

Der Bereich, in dem ein möglicher Missbrauch der persönlichen Daten stattfinden könnte und der besondere Aufmerksamkeit erfordert, ist die Überwachung und das Aufspüren von Zuwiderhandelnden. Die Identität der Fahrer muss nicht festgestellt werden, bis der Fahrer etwas getan hat, das als Verletzung der Nutzungsbedingungen des Mautsystems definiert ist oder als sonstiges Vergehen. Der Grundsatz der Verhältnismäßigkeit sollte in vollem Umfang beachtet werden, z. B. muss zunächst festgestellt werden, dass sich das Gebührensystem in dem Fahrzeug befindet und ob es fehlerfrei funktioniert. Wenn die Kontrolleinheit keine Verletzung hinsichtlich des Vorhandenseins oder der ordentlichen Funktionsweise des Gebührenerhebungsgeräts feststellt, sollte sie keine weiteren Schritte zur Ermittlung der Identität des Geräts oder des Fahrers einleiten. Nur wenn die Aufsichtsstelle feststellt, dass ein Gerät nicht vorhanden ist, dass das Gerät nicht ordentlich funktioniert oder dass die Einstellungen missbräuchlich verändert worden sein könnten, sollte eine autorisierte Stelle - im Einklang mit dem Verhältnismäßigkeitsgrundsatz - mit der Identifizierung des Fahrers fortfahren. Laut Berichten von Expertengruppen stellt die Erfassung des Nummernschilds und somit die Identifizierung des einzelnen Fahrers oder Fahrzeuginhabers eine zufriedenstellende Kontrollmöglichkeit in dieser Hinsicht dar.

Das oben Gesagte bedenkend sollten die persönlichen Daten der Fahrer, die dem System nicht zuwidergehandelt haben, auf keine Art und Weise, außer durch den Fahrer selbst, verarbeitet werden. Diesem Ansatz folgend würde die Kontrollstelle lediglich überprüfen, ob das Gerät im Fahrzeug richtig funktioniert, und nur eine autorisierte Person (für den Zweck, für den dieser Person die Berechtigung zum Zugriff auf personenbezogene Daten erteilt wurde) darf die Identität der Betroffenen erfragen oder Informationen über die Position des Fahrzeugs erhalten. Dies darf nur unter bestimmten Umständen erlaubt sein, die im Vorhinein bestimmt und aufgelistet sein müssen (z. B. wenn an dem elektronischen Mautgerät in dem Fahrzeug unerlaubte Änderungen vorgenommen wurden, wenn das Gerät auf kostenpflichtigen Straßen nicht funktioniert oder wenn das Auto gestohlen wurde). Jeder Zugriff zum Zweck der Durchsetzung auf Informationen über die Position des Fahrzeugs, die Reisezeit und Gebühren muss entsprechend dokumentiert werden, so dass eine vollständige Nachüberprüfung möglich ist. Es wäre unzulässig, einen nicht autorisierten und nicht registrierten Zugang zu den Daten in dem Gerät zu erlauben.

Die Frage der optionalen oder zwangsweisen Verwendung

Wenn die Nutzung der On-Board-Einheit optional wäre, könnten die Fahrer entweder die On-Board-Einheit oder eine andere Methode wählen, die Gebühren zu erheben und abzurechnen (z. B. Anmeldung und Zahlung an einer automatischen Station). Hervorgehoben werden muss, dass der Nutzer weder in dem optionalen noch in dem freiwilligen Schema das Gerät abschalten kann, während er auf einer kostenpflichtigen Straße fährt. Die Frage nach einer optionalen oder freiwilligen Nutzung des Mautgeräts und den Auswirkungen auf die Privatsphäre ist zu einem großen Maß eng mit der Frage der Überwachung verbunden. Im Prinzip ist die optionale Verwendung benutzerfreundlicher, weil die Betroffenen ihre vorherige Einstimmung in die Verarbeitung ihrer persönlichen Daten erteilen können; allerdings sind auch die Durchsetzungsprobleme eng mit dieser Frage verbunden und sollten insofern auch bewertet werden.

Ein Beispiel aus der deutschen Erfahrung mit Lastkraftwagen (Toll Collect System) zeigt, dass 90 % der LKW-Fahrer sich für die Installation eines Satellitensystems entschieden haben; weniger als 10 % bevorzugen andere Systeme. Die Zuverlässigkeit und Genauigkeit des installierten Systems liegt bei 99,75 %, was bedeutet, dass gewissermaßen alle Probleme in Bezug auf die Durchsetzung und Unregelmäßigkeiten bei denen auftreten, die kein Gerät installiert haben und sich bei Mautstationen anmelden und dort manuell bezahlen. Wenn man diese Erfahrungen mit LKW auf ein Mautsystem für private Fahrzeuge überträgt (insbesondere wenn dies schlussendlich auf allen Straßen eingesetzt werden soll), scheint eine optionale Verwendung wenig realistisch. Ein optionales Mautsystem im freien Verkehr würde die Installation sehr komplexer und teurer Kontrollsysteme auf allen kostenpflichtigen Straßen erfordern (Videoüberwachung, Identifizierung der Nummernschilder etc.), was im Ergebnis zu einem höheren Grad an Überwachung und einem größeren Eingriff in die Privatsphäre führen würde als ein verbindliches System. Die Entscheidung, ob man eine optionale Verwendung erlaubt oder eine verbindliche Nutzung durchsetzt, hängt wesentlich von der Größe der Implementierung und den für die Durchsetzung verfügbaren Ressourcen ab und kann daher im kleinräumigen und großräumigen Ansatz (national oder sogar international) unterschiedlich sein.[15]

Die Rechte der Betroffenen

Eine besondere Aufmerksamkeit sollte der Frage von umstrittenen Gebühren gewidmet werden. Wenn man sicherstellen will, dass personenbezogene Daten unter der alleinigen Kontrolle des Nutzers verbleiben, sollte ein Zugriff zu den Daten

[15] In den Niederlanden werden zum Beispiel alle registrierten Fahrzeuge im Land von dem Mautsystem erfasst. Es gibt allerdings Ausnahmen innerhalb dieser Gruppe: Motorräder und bestimmte Fahrzeuge wie Rettungswagen. Ausgenommene Fahrzeuge werden nicht mit einem On-Board-Gerät ausgestattet.

nur ermöglicht werden, wenn der Nutzer es ausdrücklich verlangt. Mautsysteme können und sollten so gestaltet sein, dass die detaillierten Reisedaten vollständig und dauerhaft aus dem System gelöscht werden, nachdem die Gebühren festgesetzt wurden und jede Frist, innerhalb derer die Gebühr angefochten werden kann, abgelaufen ist (wie es z. B. im Londoner City-Maut System geschieht).

Ein Fernzugriff auf die Rohdaten durch die Kontrollstelle oder durch Dritte zu anderen als Durchsetzungszwecken, unabhängig davon, ob die Daten in dem Gerät gespeichert sind oder nicht, sollte nur mit Einwilligung des Betroffenen erfolgen. Ebenso sollte die Verarbeitung zu anderen Zwecken (z. B. „pay-as-you-go"-Kfz-Versicherung oder verhaltensbasierte Werbung) nur möglich sein, wenn der Fahrzeughalter seine eindeutige und ausdrückliche Einwilligung erteilt hat.

Ergebnis

Die Arbeitsgruppe ist der Ansicht, dass die zentralisierte Verarbeitung persönlicher Daten für Mautsysteme im freien Verkehrsfluss nicht erforderlich und daher gemäß dem Verhältnismäßigkeitsgrundsatz nicht gerechtfertigt ist, angesichts der nachweisbaren Existenz technischer Lösungen, die eine zentralisierte Verarbeitung der Daten nicht erfordern. Ein starker Schutz der Privatsphäre kann und sollte von Beginn an so gestaltet sein, dass Informationen, die an die Kontrollstelle übermittelt werden, sich lediglich auf die Höhe der Gebühren beziehen und nicht auf Ort und den Zeitpunkt der Reise. Wie es in dem Bericht der National Surface Transportation Infrastructure Financing Commission der USA dargestellt wurde, würde ein solches System einen wesentlich höheren Grad an Privatsphäre bieten als andere Informationssysteme in unserer Gesellschaft, wie z. B. Kreditkarten und Mobiltelefonsysteme, bei denen der Anbieter nicht weiß, wie viel eine Person schuldet, aber wo Personen einkaufen und welche Nummern sie angerufen haben (mehr oder weniger präzise sogar den Ort). Mautsysteme können und sollten so gestaltet sein, dass detaillierte Reisedaten vollständig und dauerhaft aus dem System gelöscht werden, sobald die Gebühren festgesetzt wurden, um zu vermeiden, dass Bewegungsprofile erstellt oder die Daten zweckentfremdet werden.

Die Anonymität des Fahrers sollte innerhalb des Systems durchgängig gewährleistet bleiben. Im Hinblick auf die Durchsetzung sollte das System die Identität des Fahrers nicht feststellen, es sei denn, der Fahrer hat etwas getan, das als Verletzung der Nutzungsbedingungen des Mautsystems definiert ist. Die Verarbeitung der Daten zu anderen Zwecken (z. B. „pay-as-you-go"-Kfz-Versicherung oder verhaltensbasierte Werbung) sollte nur möglich sein, soweit der Betroffene seine eindeutige und ausdrückliche Einwilligung erteilt hat.

Im Prinzip ist die Frage nach der Privatsphäre in elektronischen Mautsystemen relativ einfach: Wesen und Zweck jedes groß angelegten Mautsystems erfordern die Verarbeitung persönlicher Daten, setzen aber nicht eine zentralisierte Verarbei-

tung der personenbezogenen Daten (solange keine Zuwiderhandlung begangen wurde), die unverhältnismäßige Verarbeitung der Daten, den Zugang zu persönlichen Daten oder eine allgegenwärtige Überwachung voraus. Die fundamentalen Grundsätze des Schutzes persönlicher Daten streben danach, die Anonymität zu bewahren; die Technologie kann und sollte in einer Weise eingesetzt werden, die es ermöglicht, die Anonymität der Fahrer zu erhalten. Jede Abweichung von diesem Grundsatz würde einen zusätzlichen Eingriff in die bereits erodierte Privatsphäre in der Informationsgesellschaft bedeuten.

45th meeting, 12th and 13th March 2009, Sofia, Bulgaria

Report and Guidance on Road Pricing

– *"Sofia Memorandum"* –

Recommendations

The Working Group recommends that the designers of large scale road pricing systems which process personal data should comply with the following recommendations designed to protect the privacy of drivers and owners of vehicles:

- The anonymity of the driver can and should be preserved by using the so-called smart client or anonymous proxy approaches that keep personal data of the drivers under their sole control and do not require off-board location record-keeping.

- Road pricing systems can and should be designed so that the detailed trip data are fully and permanently deleted from the system after the charges have been settled in order to prevent the creation of movement profiles or the potential for function-creep.

- Processing of personal data for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible with clear and unambiguous consent from the individual.

- In terms of enforcement, the system should not ascertain the identity of the driver or owner of a vehicle unless there is evidence that the driver has committed something which is defined as a violation of the road pricing system.

Background

Large-scale electronic road pricing on a »pay as you go« principle in free-flow traffic is not a new idea. Thoughts on electronic road pricing emerged in the last decades of the 20th century[1]. Different terms are used to describe the use of modern information and communication technologies in road pricing and transport, such as "electronic road tolling", "intelligent transportation systems" (ITS), "electronic toll collection", "road-user charging", "time, distance, place charging", "distance-based road user charging", "vehicle miles travelled (VMT) charging" and several others.

Existing road pricing technologies can levy a toll on highways, can charge vehicles for entering a zone, but cannot compute so-called "time, distance, place charging" algorithms required for large-scale implementations. The desired outcome of an electronic road pricing scheme is the ability to charge for *actual* use (i.e. the more you drive the more you pay) depending on the time of journey (e.g. less during off-peak periods) and with a varying tariff according to the chosen road. Traffic flow may be enhanced because drivers are not required to stop at toll booths in such schemes. In principle, this is the fairest and ecologically the most desirable way to pay, just like consumers usually pay for water or electricity consumption.

Besides road pricing, there are several other services based on time, place and distance data, such as parking schemes, pay-as-you-drive insurance, parking finder/auction, road space rationing, parking loyalty programs, congestion mapping and congestion charging, travel advisory ("you could save 12 EUR per week if you left 30 minutes earlier each day") and intelligent transport systems ("if you use A 2 motorway instead of A 3 today, you will pay 20 % less"). While electronic collection and processing of location data, identification data and charging data about individual's journeys may and is already used for several purposes and raises several socio-economic questions, this paper focuses primarily on privacy implications of (large-scale) electronic road pricing.

To have a better understanding of what the privacy implications of electronic road pricing schemes are we need to take a closer look at some of the basic principles of the system. Large-scale road pricing initiatives that involve processing of personal data (i.e. other than vignette, anonymous tag and beacon and non free-flow toll-booth based systems) are being developed all over the world, for example in the US (Oregon and Puget Sound region), Australia, New Zealand, Canada (the 407 Express Route), the Toll Collect system in Germany[2] and road pricing plans

[1] Electronic Road Charging: http://www.parliament.uk/post/pn112.pdf

[2] It has to be noted that the TollCollect system in Germany is only used for trucks: http://www.toll-collect.de

in the Netherlands[3] and Norway. Furthermore, in the EU, the aim of the Directive 2004/52/EC is to embed the "pay as you go" principle in free-flow traffic in the future European Electronic Toll Service (EETS). In its final stage of development this trans-European system should provide toll charging for all types of roads, including viaducts, tunnels and other objects. With the new road charging system, drivers could pay the toll without having to stop and cause traffic congestion. Also, the same device should be able to levy the toll on all European motorways defined as payable.

The reason road pricing is so emotive is that it brings together location data, identification data and charging data: in other words, knowing who was where at what time, and charging them for it. In order to enable the "pay as you go" principle in free-flow traffic (and also to have one interoperable system) it is clear that road pricing schemes could entail massive surveillance of the movements of individuals (vehicle owners and drivers), therefore the implications for privacy of those individuals need to be carefully studied. It is not difficult to imagine the huge value of a centralized database of driver's movement data and various function-creep scenarios where data might be exploited for purposes other than those for which the data were ostensibly collected (i.e. road pricing). Several information commissioners and data protection authorities have already issued opinions and guidance on privacy protection in electronic road pricing schemes (e.g. Ontario[4], the Netherlands, Victoria/Australia[5], New Zealand[6], Norway[7] and Slovenia[8]). Misperceptions of privacy implications are actually often considered as one of the most important deterrents for the implementation of large scale road pricing systems.

As far as technology is concerned, two mainstream technologies are envisaged for these systems: short range communications (DSRC[9]; also described as tag-beacon system) and global navigation satellite system (GNSS/CN[10]), which can

[3] Ministry of Transport, Public Works and Water Management: Implementation of road pricing system. http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/roadpricing/index.aspx

[4] 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner Ontario: http://www.ipc.on.ca/images/Resources/407-e.pdf

[5] An in-depth study of road pricing and an exhaustive list of sources were prepared by Victoria Transport Policy Institute: Road Pricing. Congestion Pricing, Value Pricing, Toll Roads and HOT Lanes. http://www.vtpi.org/tdm/tdm35.htm

[6] Road Reform and Privacy: Which Way Forward? Submission by the Privacy Commissioner to the Ministry of Transport in relation to the final report of the Roading Advisory Group: http://www.privacy.org.nz/road-reform-and-privacy-which-way-forward/?highlight=impact

[7] http://www.curacaoproject.eu/documents/newsletter-issue3.pdf

8 http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=568

[9] DSRC – Dedicated Short Range Communications.

[10] GNSS/CN – Global Navigation Satellite System/Cellular Networks

determine the position of the car and transmit the data via high-performance wireless communication networks – the latter is frequently referred to as satellite road pricing system.

Each has its advantages and disadvantages: the DSRC-based solutions technologies, for example, are more widely used and have been more frequently tested but they are not suitable for all roads[11]. The choice of technology depends significantly on the implementation size and differs between relatively small-scale (e.g. metropolitan[12]) and large scale (nationwide or even international wide) implementation. Speaking from the viewpoint of large-scale implementations the DRSC-based solutions seem to be losing ground. Due to the enormous number of road segments to cover, solutions requiring substantial roadside infrastructure to determine the amount of road usage – as in existing DSRC-based systems – are less suited in cases where all roads are likely to be charged[13], a view which is also echoed in the recent report from the US National Surface Transportation Infrastructure Financing Commission[14]. The advantage of a satellite-based system is its flexibility, while on the other hand such systems have not been tested widely in practice.

The exploitation of electronic road pricing schemes is – leaving aside the vast socio-economic debates and consequences – often hampered by two common privacy misperceptions held by the general public and media that need to be firmly discarded.

Firstly, the Working Group emphasizes that there should be no concern that GPS-based approaches would mean building of an all encompassing database on the position of vehicles in a "big brother in the sky" style. The US GPS, Russian GLONASS as well as the future Galileo satellite positioning systems are based on passive receivers, which only calculate the location of the vehicle using satellite data, and these receivers cannot communicate the information on the location of the car back to the satellites. Therefore, in opting for a system of satellite-based road charging we need to understand that by satellite navigation a vehicle only obtains the information on its position, whilst the location data is transmitted to the control toll charging centre via wireless networks, such as for example the GSM network. An all encompassing database of location and identification data could therefore only exist "on the ground" in the control centres, which is exactly what this paper is dealing with.

---

[11] Privacy-Sensitive Congestion Charging. Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle: http://www.cl.cam.ac.uk/~arb33/papers/BeresfordDaviesHarle-PrivacyAwareCongestion-SPW2006.pdf

[12] Singapore, Melbourne, Trondheim, Toronto are examples of metropolitan-scale systems.

[13] Privacy And Distance Based Charging For All Vehicles On All Roads. Stefan Eisses, Wiebren de Jonge and Vincent Habers: http://www.tipsystems.nl/files/Privacy_and_RUC_ITSLondon-doc.pdf

[14] National Surface Transportation Infrastructure Financing Commission: Paying Our Way, a New Framework for Transportation Finance, February 24, 2009: http://www.itif.org/index.php?id=227

Secondly, comparisons are frequently made with mobile telephony or credit cards, where individual's data is or may be tracked. The Working Group would like to point out that such simple comparisons are not appropriate, foremost because road pricing devices must remain in constant operation (at least on payable roads), unlike in the case of mobile phones the use of which is entirely voluntary. The ability to switch off the device on a payable road would facilitate payment evasion, and for this reason the privacy implications of road pricing schemes become even more relevant.

The distribution of the charging process

The charging process is split into four phases:

1. determining the position of the vehicle,
2. determining the segment of the road or toll element and the corresponding tariff,
3. calculating the amount due for that segment,
4. calculating the total amount due for the journey.

A crucial factor when estimating privacy implications is how the phases of the charging process are distributed between different data processors. The four phases of the charging process can either be performed by one processor or they can be split between two or more of them. Consequently the privacy implications differ from one implementation model to another. Some of the models are presented below together with the most important elements that need to be considered when assessing privacy implications. The two principal models for road pricing are the **thin client approach** and the co-called **smart client** approach; however other models exist in between those two, such as the distributed role approach and proxies. These four approaches are discussed below

The thin client approach

The least favoured solution for electronic road pricing system, in terms of privacy protection, is where all data on journey time and position of vehicles are sent to or collected by a single body or institution acting as a control centre. The so-called thin client (or On-Board Unit – OBU) only collects the data on journeys travelled and all four phases of the charging process are processed by the control centre using a centralized database of location data, identification data and charging data.

The Working Group expresses its concerns about adopting this approach, since it clearly offers the least protection for the privacy of the individuals. In principle,

the question of preferring thin or smart clients is a question of centralized vs. distributed processing, a dilemma often encountered in privacy and data protection.

The proponents of centralized processing claim that if data were kept centrally and protected by suitable data security mechanisms (e.g. appropriate access control, logging of personal data processing etc.), it would be possible to ensure a higher level of security than a single individual could ensure. A counterargument however is that where the data are under the control of an individual, only his/her own personal data remain vulnerable (e.g. if the vehicle or the road pricing on-board device was stolen), whereas in the centralised processing system personal data of all individuals are potentially vulnerable (despite a possibly higher level of security). For this reason, and from the viewpoint of privacy protection, it is necessary to favour those solutions where personal data are not kept centrally, but remain in the possession and under control of an individual. Furthermore, privacy advocates are frequently dealing with the so-called function creep phenomenon, where data originally collected for one purpose (which can be perfectly legitimate and lawful) is later used for another purpose, where access to data is possible by previously unforeseen third parties and so on. Function-creep worries practically vanish when data are processed under the control of the user.

The distributed-role approach

Some models propose the so-called distributed-role approach, which supposedly provides for better protection of privacy and personal data. The distributed-role approach is a solution based on the principle of sharing the data between two centres or parties, one of them having location and charging data whereas the other only has identification data of drivers.

The first centre or party has the identification number of the device in the vehicle and receives information on the route the vehicle has made (journey time and position), but does not know who the owner of the device is. Based on this information the centre calculates the fees due. Such aggregated calculations of data (only the sum of the toll within a certain time period, without information on journey time and position), are then sent together with the identification number of the device to another centre which can identify the owner of the device who is then charged with the toll, however, this second centre does not keep the information on the journey of the vehicle. The proponents of this approach often claim that this distribution of roles does not entail that personal data are processed; however the Working Group would challenge such reasoning, because a vast amount of personal data is still being processed by the centres.

This solution only apparently protects the privacy of an individual, even though one centre keeps the information on the vehicle positions and journey time and

does not know the identity of the driver, and vice versa. Throughout this approach enormous amounts of personal data are still collected and processed centrally by one centre and only the identification data is trusted with another centre or party. The Working Group would like to echo the opinion of the Article 29 Working Party that data, relating to an identified or identifiable natural person, need to be treated as personal data and that the identifiability of an individual is not assessed only through the means and resources of a data controller (in this case the first centre) but should rather be assessed more generally. The controller should anticipate that the "means likely reasonably to be used" to identify the persons will be available e.g. through the courts appealed to (otherwise the collection of the information makes no sense), and therefore this information should be considered as personal data. Regardless of whether the first centre can or cannot identify an individual to whom the data on time and position refer to by itself, this centre undoubtedly processes personal data. To support this, it is evident that in case the road charges have not been paid, or the person has refused payment, the creditor will need to find a quick and simple way to reproduce the calculation of the toll which means that the data on journey time and position of an identifiable person will need to be processed. Furthermore, the function creep effect is again quite possible since large amounts of data are centrally stored.

The smart client approach

In order to ensure the privacy of individuals, clearly the most appropriate system would be the one in which the data needed for the purpose of road pricing, would be exclusively under the control of the user. In this case the calculation of the toll would be made by the device (the so called intelligent device), while the control centre would receive only the sum of the toll incurred. This means that all four phases of the charging process in electronic road pricing system would be processed by the device itself: determining the position of the vehicle, determining the segment of the road and the corresponding tariff, calculating the amount due for that segment, and calculating the total sum.

The anonymity of the driver would thus be preserved since all the data on the position and journey time would be kept under the sole control of the user. The users should only identify themselves if certain irregularities emerged in which identification would be required: for example, when the user has not paid a correctly calculated toll fee, or when the vehicle has been stolen, when the user's toll system device is broken down or malfunctioning (whilst driving on a chargeable road segment). The control centre only needs to be sure that the device in the vehicle which calculates the toll is working correctly on the roads on which tolls are charged.

In such a system the control centre does not have data on the position of the vehicle; it only checks whether the device is operating correctly. This system, of

course, also requires some operational measures such as protection of the equipment from fraud (including jamming, tampering, shielding, tweaking, intentional malfunctioning etc.) One very important aspect of both thin and smart clients is that they cannot be switched off by the user when the car is on a payable road, since this would enable payment evasion. The smart client approach does not come without challenges - it is for example necessary to provide suitable certification standards, proper installation and maintenance of such devices, and also consider some other technical aspects (e.g. power supply, checking correct functioning, memory capabilities), and probably the most important aspect – the costs.

While the smart client approach appears to be a more costly solution than the so-called thin client, the smart client approach also has certain economic advantages: the »intelligent« device is not sensitive to communication hindrances (e.g. areas which are not covered by GSM signal), or if the control centre is temporarily not operating since the system can process the toll itself. On the other hand, the device which continuously sends data (the thin client) to the control centre and relies on control centre's calculations cannot process the calculations of the toll by itself in the areas with poor GSM coverage, or when the central control is not working. It is also very important to mention that the intelligent device also supports operation in the thin client mode (metaphorically speaking the "dumb" client cannot become "smart" whereas vice-versa is possible), which is an especially important requirement when interoperability is needed (e.g. within the future European Electronic Toll Service) or with other pre-existing metropolitan toll collection or congestion charging systems. The devices in vehicles will need to know how to respond to different regimes: after entering the territory of another operator, the device will receive instructions on how to work. International standardisation organisations (ISO and CEN) are developing suitable technical standards, whilst the industry already has proven working solutions. While economic factors are clearly crucial for take-up of a certain system, they do not affect the privacy implications. The perceived cost penalty for a smart client could be minimised by mass production economies or incentives (e.g. by bundling an onboard hands-free mobile phone or satellite navigation system into the device).

A smart client could also facilitate anonymous use if pre-pay options, as currently provided for mobile phones, were offered. A driver should have the opportunity to buy toll credits which could be applied to the onboard unit, which could then advise the control centre that the charges for the payable road segment in question had been pre-paid.

Proxies

Other mixed-type approaches have also been known and are already available on the market. The charging centre can, for example, operate merely as a technical centre – a kind of an intermediate or proxy which has been selected to perform

calculations. These proxies (usually dubbed as anonymous forwarding proxies or anonymous loop-back proxies) can be on or off-board and can have the functionality to store data on-board or not. Assessing the privacy implications of these approaches is in principle a matter of trust (i.e. whether the device can be trusted and whether the control centre or third parties are really unable to access personal data).

The Working Group is generally in favour of such proxy approaches provided that their privacy protection can be independently assessed and they meet the privacy protection level of a purely smart-client approach.

Enforcement

Enforcement is another crucial element that needs to be designed in a privacy friendly manner if we are to preserve the anonymity of the drivers in electronic pay-as-you-go road pricing schemes.

The area where possible abuse of personal data may happen, and requires special attention, is the implementation of surveillance and detection of offenders. The identity of the drivers must not be ascertained unless there is evidence that the driver has committed something which is defined as a violation of the road pricing terms of use or some other offence. The principle of proportionality should be fully respected, i.e. first of all it needs to be established whether the toll system device is present in the vehicle and whether it functions faultlessly. If the control unit does not detect any violations regarding the presence or proper functioning of the toll charging device, it should make no further steps for the identification of the device and the driver. Only if the supervising unit detects absence of the device, improper functioning of the device, or that some improper adjustments on the device may have been made, should the authorised body, according to the principle of proportionality, proceed with identification of the driver. According to reports of expert groups, number plate recognition process and thus identification of the individual driver or owner is an satisfactory method of control in this respect.

Considering all the above, the personal data of drivers who have not committed any offence should not be processed in any way except by the driver. Using this approach, the control centre would only check if the device in the car is functioning correctly, and only an authorised person (for the purpose for which this person has been given authorisation to access personal data) may request identification of the individual, or obtain information on the position of the vehicle. This may be permitted only in certain circumstances which need to be predefined and enumerated (for example if the electronic road pricing device in a car has been tampered with, or if the device was not working while using payable roads, or if the car was stolen). Every access to the information on the position, journey time and tolls for

enforcement purposes needs to be suitably recorded, allowing an authentic and complete auditing tracing. It would be impermissible to allow unauthorised and unregistered access to the data in the device.

The question of optional or compulsory use

If the usage of an on-board unit is optional, the drivers can either use an on-board unit or choose a different method of toll charging and payment (e.g. by subscribing and paying the toll on an automatic station). What needs to be stressed is that in either optional or compulsory scheme the user cannot switch off the device while driving on a payable road. The question of optional or compulsory use of the road pricing device and the impact on privacy is to a great extent closely related with the question of surveillance. In principle, optional use is more user-friendly since individuals can give prior consent to processing of their personal data; however the enforcement issues are closely connected and should be evaluated as well.

An example from German experience for heavy vehicles (the TollCollect system) shows that 90 % of truck drivers have opted for the installation of a satellite toll system and less than 10 % prefer other systems. Reliability and accuracy of the installed systems is 99.75 %, which means that virtually all problems of enforcement and irregularities occur with those without installed devices who subscribe and pay manually at toll stations. If we transfer this experience from heavy vehicles to a road pricing system for private cars (especially if it is to be eventually used on all toll roads), optional use seems less realistic. An optional road pricing system in free flow traffic would require installation of very complex and expensive control systems on all payable roads (video surveillance, identification of number plates, etc.), which would consequently mean a high degree of surveillance and even greater encroachment into the privacy than in a compulsory system. The decision on whether to allow optional use or enforce compulsory use largely depends on the implementation size and enforcement resources and might differ in a small-scale and a large scale (nationwide or even international wide) approach[15].

Data subjects rights

Special attention should be paid to the questions of disputed charges. If we want to ensure that personal data remain fully under the user's control, access to the

[15] In the Netherlands for example all vehicles registered in the country will be covered by road pricing. There are, however, exemptions within this group: motorcycles and certain vehicles, such as emergency services. Exempted vehicles will not be fitted with an on-board unit.

data should only be provided for if the user explicitly requests so. Road pricing systems can and should be designed in a way that the detailed trip data are fully and permanently deleted from the system after the charges have been settled and any period for disputing the charges has expired. (e.g. as happens in the London congestion charge system)

Remote access to raw data by the control centre or by third persons for purposes other than enforcement, regardless of whether the data are stored in the device or not, should only be allowed upon consent of the individual. Similarly, processing for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible if the vehicle owner has given his clear and unambiguous consent.

Conclusions

The Working Group is of the opinion that centralized processing of personal data for the purposes of road pricing in free-flow traffic is not necessary and is therefore unjustified under the principle of proportionality, given that proven technological solutions exist that do not require centralized processing of personal data. Strong privacy protection can and should be designed from the start so that the information transmitted to the control centre would only relate to the bulk charges due and would not include detailed data on time and place of travel. As pointed out in the report by the US National Surface Transportation Infrastructure Financing Commission, such a system would provide considerably more privacy than other information technology systems in our society, such as credit card and mobile phone systems, where the provider knows not just how much a person owes but where the individual made purchases and what phone numbers were called (more or less precisely even the location). Road pricing systems can and should be designed so that the detailed trip data are fully and permanently deleted from the system after the charges have been settled in order to prevent the creation of movement profiles and the function-creep effect.

The anonymity of the driver should be preserved throughout the functioning of the system. In terms of enforcement the system should not ascertain the identity of the drivers unless the driver has committed something which is defined as a violation of the road pricing system. Processing of personal data for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible with clear and unambiguous consent from the individual.

In principle, the question of privacy in electronic road pricing systems is quite simple: any large scale road pricing system in its essence and purpose does require personal data processing but does not require centralised personal data processing (so long as no offence has been committed), nor does it require dispro-

portionate processing of personal data, access to personal data and ubiquitous surveillance. The fundamental principles of personal data protection strive for maintaining the anonymity of the driver and technology should and can be used in a way that preserves the anonymity of the driver. Any digression from this principle would represent an additional encroachment into already eroded privacy in the information society.

Empfehlung zum Datenschutz und Elektronik-Abfall („E-Waste“)

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation,

Berücksichtigend, dass die zunehmende und umfassende Nutzung elektronischer Geräte und Anlagen sowohl für private als auch für öffentliche Zwecke die Notwendigkeit mit sich bringt, solche Einrichtungen auch angemessen zu entsorgen und/oder zu recyceln;

Berücksichtigend, dass solche elektronischen Geräte und Anlagen Einrichtungen zur Kommunikation enthalten und in Anbetracht der zunehmenden technischen Konvergenz und des Vorhandenseins von Mehrzweckgeräten[1];

Berücksichtigend, dass die Europäische Union seit langem eine umweltfreundliche Politik verfolgt, die die Verminderung der Ausbeutung natürlicher Rohstoffe sowie Maßnahmen zur Verminderung der Verschmutzung umfasst; und berücksichtigend, dass solche Ziele auch seit langem in verschiedenen Nicht-EU-Staaten verfolgt werden;

Berücksichtigend, dass die angesprochenen Strategien angemessene Recycling- und Abfallbeseitigungsmaßnahmen in Bezug auf Elektro- und Elektronikabfall (E-Waste) vorsehen, wie sie mit der EG der Richtlinie 2002/96/EG[2] auf den Weg gebracht wurden;

Berücksichtigend, dass es einschlägigen regulatorischen Instrumenten bisher weder auf nationaler noch auf überstaatlicher Ebene gelungen ist, den Risiken, die mit dem Recycling oder der Beseitigung von Elektro- und Elektronik-Geräten insoweit einhergehen, dass solche Geräte persönliche Daten über den Nutzer des Geräts oder Dritte enthalten können, hinreichend Rechnung zu tragen;

---

[1] Abgesehen von und über solche Geräte und Ausstattungen hinaus, die ursprünglich für Kommunikationszwecke bestimmt waren, gibt es eine zunehmende Anzahl an Geräten, die als Datenübertragungsendgerät eingesetzt werden können, wenn sie an ein elektronisches Kommunikationsnetzwerk angeschlossen sind.

[2] Richtlinie 2002/96/EG des Europäischen Parlaments und des Rates vom 27.Januar 2003 über Elektro- und Elektronik-Altgeräte.

Berücksichtigend, dass es notwendig ist, die Aufmerksamkeit aller Interessenvertreter – sei es im öffentlichen oder im privaten Bereich – inklusive solcher staatlichen Stellen und Firmen, die die E-Waste recyceln oder verwerten, auf dieses Thema zu lenken, insbesondere insoweit, als dass diese Stellen, vor allem diejenigen, die sich selbst Kommunikationsgeräte und -Ausstattungen zunutze machen, als datenverarbeitende Stellen verpflichtet sind, angemessene Maßnahmen zu ergreifen, um die Sicherheit persönlicher Daten zu gewährleisten, wobei diese Maßnahmen zum Zeitpunkt des Recycelns und/oder des Beseitigens derjenigen Geräte und Ausstattungen, die zur Verarbeitung persönlicher Daten eingesetzt wurden, durchgeführt werden müssen;

Unter Bezugnahme auf generelle bestehende Leitlinien, wie sie von manchen nationalen Datenschutzbehörden in Verbindung mit der angemessenen Vernichtung und/oder Löschung von persönlichen Daten aufgestellt wurden[3];

EMPFIEHLT

1. Dass die nationalen Regulierungsbehörden, in Zusammenarbeit mit den nationalen Datenschutzbehörden und allen relevanten Interessenvertretern aus der Industrie, angemessene Maßnahmen auf den Weg bringen, die den unberechtigten Zugang zu persönlichen Daten, die in zu recycelnden und/oder zu verwertenden Geräten gespeichert sind, verhindern oder begrenzen. Darüber hinaus muss sichergestellt werden, dass die entsprechenden Maßnahmen auch von den datenverarbeitenden Stellen umgesetzt werden. Solche Maßnahmen könnten zum Inhalt haben, dass Informationstechnik und/oder andere Werkzeuge und/oder Vorkehrungen – soweit als möglich als Freeware (kostenlose und lizenzfreie Software) – bereitgestellt werden, um die Speicherung personenbezogener Daten in den entsprechenden Geräten zu begrenzen oder zu verhindern, da es sich als schwierig erweisen wird, solche Daten zu entfernen, ohne das betreffende Gerät und/oder Equipment zu zerstören[4];

[3] Vgl. z. B.: Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe „Sicheres Löschen magnetischer Datenträger". Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes, Stand: 7.10.2004 (http://www.datenschutz.mvnet.de/dschutz/informat/magloe/magloe.html); Orientierungshilfe „Datensicherheit bei USB-Geräten", Stand: November 2003 (http://www.datenschutz.mvnet.de/dschutz/informat/usb/oh_dsusb.html); Hellenic Republic Data Protection Authority, Directive 1/2005, Athens 17-10-2005, Ref. Num. 3845; Entscheidung der Italienischen Datenschutzbehörde vom 9. Dezember 2008, abrufbar unter: http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482 ; siehe auch: Pressemitteilungen des Berliner Beauftragten für den Datenschutz und die Informationsfreiheit vom 24. Januar 2007 (http://www.datenschutz-berlin.de/content/nachrichten/pressemitteilungen/pressemitteilungen-im-jahr-2007) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 23. Dezember 2008 (http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM_37_08_KeinePersoenlichenDatenAufAusrangiertenPCsVergessen.html?nn=409394).

[4] In dieser Hinsicht kann auf herausnehmbare Speicherkarten verwiesen werden, wie sie in Mobiltelefonen eingesetzt werden.

2. Dass die Maßnahmen zum Schutz personenbezogener Daten, die von den datenverarbeitenden Stellen zu ergreifen sind, den unterschiedlichen Risiken Beachtung schenken, die mit Recyclingprozessen im Gegensatz zu Abfallbeseitigungsmaßnahmen von Elektronik-Abfall einhergehen.

3. Dass mit der Einführung von Maßnahmen zum Schutz persönlicher Daten in Verbindung mit dem Recycling von Elektronik-Abfall insbesondere sichergestellt werden muss, dass die personenbezogenen Daten von magnetischen und elektronischen Medien unter Einhaltung des gegenwärtigen Stands der Technik, wie zum Beispiel durch mehrfaches Überschreiben oder Entmagnetisierung (degaussing), gelöscht werden;

4. Dass bei der Einführung von Maßnahmen zum Schutz personenbezogener Daten in Verbindung mit dem Recycling von Elektronik-Abfall die Zweckmäßigkeit der Implementierung effektiver Mechanismen zur Zerstörung magnetischer und elektronischer Medien berücksichtigt werden soll, um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern;

5. Dass die zuständigen nationalen und supranationalen Stellen angemessene Aufklärungsmaßnahmen ergreifen, um die datenverarbeitenden Stellen und die Nutzer über die einschlägigen Risiken und Anforderungen zu informieren.

Recommendation

on Data Protection and E-Waste

The International Working Group on Data Protection in Telecommunications,

Considering that the increasingly widespread use of electronic devices and equipment for both private and public purposes entails the need for such equipment be adequately disposed of and/or recycled;

Considering that such electronic devices and equipment include electronic communications tools, by also having regard to the increasing technological convergence and the availability of multi-purpose devices;[1]

[1] Apart from and beyond devices and equipment that have been conceived originally to serve communication purposes, there is an increasing array of devices that can work as communication terminals when connected with an electronic communications network.

Considering that the European Union has long been pursuing an environmentally-friendly policy including reduced exploitation of natural resources and measures to prevent pollution; considering, in addition, that such policies have long been pursued also in several non-EU countries;

Considering that the policies in question envisage appropriate recycling and disposal measures in respect of electric and electronic waste (e-waste), as set forth in the EU via directive 2002/96/EC[1];

Considering that the applicable regulatory instruments at both national and supranational level have failed so far to take due account of the risks inherent in the recycling and/or disposal of electrical and electronic devices to the extent such devices may contain personal data relating to the users of those devices and/or to third parties;

Considering that it is necessary to draw all the stakeholders' attention – whether in the public or in the private sector, including governmental authorities and companies dealing with the recycling and/or disposal of e-waste – to the circumstance that all data controllers – in particular those availing themselves of communications devices and equipment – are required to take appropriate measures to ensure the security of personal data, and that such measures should also be implemented at the time of recycling and/or disposing of equipment and devices used to process personal data;

Taking account of existing guidance as developed more generally by some national Data Protection Authorities in connection with the appropriate destruction and/or erasure of personal data[2];

[1] Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment (WEEE).

[2] See, e.g., Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe "Sicheres Löschen magnetischer Datenträger". Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes Stand: 7.10.2004 (http://www.datenschutz.mvnet.de/dschutz/informat/magloe/magloe.html); Orietntierungshilfe "Datensicherheit bei USB-Geräten", Stand: November 2003 (http://www.datenschutz.mvnet.de/dschutz/informat/usb/oh_dsusb.html); Hellenic Republic Data Protection Authority, Directive 1/2005, Athens 17-10-2005, Ref. Num. 3845; decision by the Italian data protection authority dated 9 December 2008, available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482 ; see also the Press Releases by then Berlin Commissioner for Data Protection and Freedom of Information of 24 Januar 2007 (http://www.datenschutz-berlin.de/content/nachrichten/pressemitteilungen/pressemitteilungen-im-jahr-2007) and by the German Federal Commissioner for Data Protection and Freedom of Information on 23 December 2008 (http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM_37_08_KeinePersoenlichenDatenAufAusrangiertenPCsVergessen.html?nn=409394).

RECOMMENDS

1. that the domestic regulators, in co-operation with national Data Protection Authorities and all the relevant industry stakeholders, set forth the appropriate measures to prevent or limit unauthorised access to the personal data stored in electric and electronic equipment that is intended for recycling and/or disposal, and ensure that the measures in question are implemented by data controllers. Such measures might include making available IT and/or other tools and/or arrangements, where possible via freeware, to prevent or limit storage of personal data in the given device and/or equipment, as it might prove difficult to remove such data without destroying the said device and/or equipment[3];

2. that the personal data protection measures to be adopted by data controllers in connection with e-waste take account of the different risks related to recycling as opposed to disposal of e-waste;

3. that in adopting data protection measures in connection with recycling of e-waste, account be taken, in particular, of the need to ensure actual erasure of the personal data from magnetic and electronic media in compliance with state-of-the art technical standards such as multiple-pass overwriting or demagnetization (degaussing);

4. that in adopting data protection measures in connection with disposal of e-waste, account be taken of the advisability to implement effective destruction procedures of magnetic and electronic media so as to prevent unauthorised access to personal data;

5. that adequate awareness-raising initiatives be taken by the competent national and supranational authorities to inform data controllers and users at large about the relevant risks and requirements.

[3] Reference can be made in this regard to removable memory sticks used in cell phones.

46. Sitzung, 7. und 8. September 2009, Berlin

Arbeitspapier zu Risiken für die Privatsphäre im Zusammenhang mit der Wiederverwendung von Email-Accounts und ähnlichen Diensten der Informationsgesellschaft

– überarbeitet und aktualisiert auf der 47. Sitzung, 15./16. April 2010, Granada, Spanien –

Einleitung

Für viele Menschen sind Emails das primäre Kommunikationsmittel geworden, das traditionelle Briefe sowohl für private als auch für geschäftliche Zwecke ersetzt. Bei einem Email-Account, der eine Person identifizieren und für private Kommunikation genutzt werden kann, handelt es sich nach allgemeiner Auffassung der Datenschutzbehörden um personenbezogene Daten.

Eine Person kann einen oder mehrere Email-Accounts haben, die über einen kostenlosen oder kostenpflichtigen Dienst angeboten werden; einem Angestellten kann es auch von seinem Arbeitgeber gestattet sein, eine geschäftliche Email-Adresse für private Zwecke zu nutzen. Email-Accounts, die scheinbar umsonst zu haben sind, können mit anderen Informationsdiensten, wie Breitbanddiensten und Kabelfernsehen gebündelt sein.

Was also geschieht, wenn eine Person ihren Email-Anbieter wechseln muss?

Die Analogie in der realen Welt besteht darin, aus einem Haus in ein anderes umzuziehen. Gewöhnlicherweise schicken Personen, die umziehen, Briefe an alle ihre geschäftlichen und privaten Kontakte, um diese über den Umzug zu informieren. Darüber hinaus wird die Person in der Regel mit dem Post-Zusteller vereinbaren, dass alle Briefe an die neue Adresse weitergeleitet werden – heutzutage keine einfache Angelegenheit, da viele Postzustellungsunternehmen eingebunden sein können. Die Lösung kann darin bestehen, den neuen Bewohnern für die verbleibende Post Etiketten mit der neuen Anschrift zu geben.

Wenn wir diese Analogie aus der echten Welt in die virtuelle Welt übertragen, müssen wir alle Dienste der Informationsgesellschaft in Betracht ziehen, die es mit sich bringen, eine Person anhand des Namens zu identifizieren. Dies kann die zunehmend beliebten sozialen Netzwerke umfassen und auch Accounts bei virtuellen Marktplätzen, die eine Email-Adresse zu Zwecken der Validierung nutzen und an die elektronische Güter und Belege etc. gesendet werden können. Dassel-

be Problem könnte sich auch im Fall des Verschickens von SMS im Zusammenhang mit Mobiltelefonen ergeben.

Wechsel einer Email-Adresse oder eines Accounts bei Diensten der Informationsgesellschaft

Wenn eine Email-Adresse oder ein virtueller Account geschlossen wird, besteht die Möglichkeit, dass ein neuer Nutzer den Benutzernamen wieder benutzen und dessen „Vergangenheit erben" könnte. Diese Möglichkeit ist im Fall von kostenlosen „email-for-life"-Diensten (sowie bei gmail oder hotmail) ziemlich abwegig, da solche Anbieter kaum abgelaufene Accounts neu verteilen würden.

Außer wenn der Nutzer für eine Domain gezahlt hat, wird der Domain-Name aller Wahrscheinlichkeit nach mit dem Service-Provider verbunden und nicht von einem auf den anderen Anbieter übertragbar sein.

Beispielhaft muss man sich jemanden vorstellen, der einen sehr gebräuchlichen Namen hat, wie „Joe Doe", der in Portugal lebt, gmail benutzt, sich bei einem Kabelfernsehkanal anmeldet und für eine Firma namens Xpto arbeitet; Joe könnte mehrere Email-Accounts haben, wie z. B. **joedoe99@gmail.com**, **joedoe@cabletv.pt**, **joedoe@xpto.pt**. Zusätzlich könnte er eine persönliche Domain für seine Familie gekauft haben oder nutzen wie **doe.pt** und die Email-Adresse **joe@doe.pt** benutzen.

Wenn er seinen gmail-Account aufgeben möchte, kann er ziemlich sicher sein, dass sein Account **joe.doe99@gmail.com** nicht wieder vergeben wird, aber wenn er das Abonnement für das Kabelfernsehen beendet oder seinen Arbeitsplatz wechselt, dann wird er vielleicht entdecken, dass er nicht mehr in der Lage ist, auf seine Emails über die Accounts **joedoe@cabletv.pt** oder **joedoe@xpto.pt** zuzugreifen.

Auf der anderen Seite sollte die Domain **doe.pt** nicht ohne Weiteres auf einen anderen übertragbar sein, vorausgesetzt, seine Familie zahlt weiter dafür.

Wenn dagegen sein früherer Kabelfernsehanbieter einen neuen Kunden hat und sein früherer Arbeitgeber einen neuen Angestellten, der auch Joe Doe heißt, könnten sie entscheiden, seine alte Email-Adresse an diese neue Person zu vergeben. In diesem Fall wird der neue „Inhaber" wohl Email-Nachrichten und persönliche Information „erhalten", die an den ursprünglichen Inhaber gerichtet waren.

In gleicher Weise kann jeder neue Besitzer einer wieder vergebenen Domain, bei der die Bezahlung ausgelaufen ist, Email-Verkehr erhalten, der an den früheren Besitzer gerichtet ist.

Mögliche negative Folgen

Dies kann zahlreiche negative Folgen haben:

- Wenn der Nutzer Abonnements für Email-Newsletter nicht kündigt oder nicht alle Kontakte über den Wechsel seiner Adresse informiert hat, wird der neue Besitzer Informationen erhalten, die für den früheren Besitzer bestimmt sind, was zur Preisgabe personenbezogener Daten führt;

- Wenn ein Nutzer die „Passwort-vergessen"-Option eines Dritten nutzt, bei dem er sich unter der alten e-mail-Adresse registriert hat, würde der neue Besitzer seinen Nutzernamen und das Passwort für diese website erhalten;

- Wenn ein Beschäftigter seine Arbeitsstelle verlässt, könnte der neue Beschäftigte persönliche Nachrichten erhalten, die für den ehemaligen Beschäftigten bestimmt sind, sowie auch geschäftliche Emails für denjenigen, der den ehemaligen Beschäftigten ersetzt hat;

- Wenn der Vertrag mit einem Internet-Service-Provider beendet wird, könnte sich der neue Kunde versehentlich oder absichtlich als der ehemalige Inhaber der Email-Adresse ausgeben.

Ähnliche Erwägungen sind auf andere Dienste der Informationsgesellschaft anwendbar, wie z. B. Instant Messaging, VoIP/Internettelefonie und soziale Netzwerke, besonders wenn die Email-Adresse zur Authentifizierung genutzt wird. Wenn ein Benutzer einen Dienst beenden möchte, kann der neue Benutzer Nachrichten empfangen, die für den ehemaligen Nutzer bestimmt sind, oder – was schwerwiegender ist – versuchen, als der alte Benutzer aufzutreten.

Während die mobile Rufnummernmitnahme (mobile number portability – MNP), die Möglichkeit des Auftretens dieses Problems im Zusammenhang mit Mobiltelefonen reduzieren kann, mag die Möglichkeit zur Rufnummernmitnahme nicht immer verfügbar sein (z. B. im Fall von mangelndem Bewusstsein, Umzug in ein anderes Land, Tod des Nutzers oder bei manchen Formen von „pay-as-you-go"-Diensten). Dann besteht wieder die Möglichkeit, dass jemand anders eine kürzlich verwendete Rufnummer und das damit verbundene Erbe an SMS-Nachrichten übernimmt.

Dies ist deshalb besonders problematisch, weil SMS in der Regel in besonders vertraulichen Bereichen wie Online-Banking und E-Ticketing verwendet werden.

Obwohl die Portabiliät von Mobilfunknummern geholfen hat, diese Probleme zu behandeln, könnte der Benutzer das Gefühl haben, dass er seine Email-Adresse oder die Nummer seines Mobiltelefons, einen bestimmten Internet-Service-Pro-

vider oder Mobilfunkanbieter für immer behalten muss, um seine Privatsphäre und persönliche Sicherheit zu wahren.

Empfehlungen

Die Arbeitsgruppe hat sich schon früher mit Aspekten des Schutzes der Privatsphäre und der Sicherheit im Zusammenhang mit Telekommunikationsdiensten[1], Internetdiensten[2] und sozialen Netzwerken[3] beschäftigt.

Die Arbeitsgruppe ist der Auffassung, dass ein Anbieter von Diensten der Informationsgesellschaft (im Folgenden als „ISP" bezeichnet) Dienste anbieten sollte, die es dem Nutzer ermöglichen, jede schädigende Konsequenz, die aus der Kündigung des Vertrages resultieren könnte, zu minimieren, und gibt folgende Empfehlungen:

1. Der ISP sollte eine Übergangsphase von mindestens drei Monaten vorsehen, bevor irgendjemand die Email-Adresse, persönliche Domain oder Telefonnummer eines vormaligen Nutzers übernehmen kann.

2. Der ISP sollte dem Nutzer eine Möglichkeit bieten, dass für die Dauer der Übergangsphase Nachrichten, die an die ausgesetzte Email-Adresse oder Nummer geschickt werden, zusammen mit einer passenden automatisierten Nachricht zurückgesandt werden.

3. Der ISP sollte einen Warnhinweis anbieten, der den Nutzer über das mit dem Ende des Vertrags verbundene Risiko, seine Email-Adresse zu verlieren, informiert sowie über die mögliche Preisgabe von Daten.

4. Der ISP könnte eine Funktion wie einen „wandernden" Ordner anbieten, in dem der Nutzer die Login-Daten speichern könnte, die für Web-Dienste verwendet werden, bei denen er sich unter Nutzung seiner e-mail-Adresse oder Mobilfunknummer registriert hat. Wenn der Account geschlossen oder der Vertrag beendet wird, könnte er den Ordner zu einem anderen Dienst mitnehmen, oder er hätte wenigstens eine Liste aller Dienste Dritter, mit denen seine e-mail-Adresse oder Mobilfunknummer verbunden ist, und könnte die e-mail-Adresse oder Mobilfunknummer dort ändern. Dies würde erfordern, dass der Nutzer solche Informationen stets aktualisiert.

---

[1] Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz (Berlin 13./14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

[2] Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP) (Berlin 5/6.09.2006); http://www.datenschutz-berlin.de/attachments/101/WP_VoIP_de.pdf?1201702122

[3] Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – Rom Memorandum – (Rom 3/4.03.2008); http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf?1234867489

5. Dienste, die eine SMS-Authentifizierung verwenden (z. B. Online-Banking), sollten die Mobiltelefonnummer anzeigen, an die die Nachricht verschickt wurde. Wenn der Dienst innerhalb eines gewissen Zeitraumes keine Rückmeldung von dem Nutzer erhält, dass die Transaktion fortgeführt werden soll, sollte die betreffende Nummer als gefährdet eingestuft und so lange ausgesetzt werden, bis der Inhaber der Accounts erneut die Nummer des zu verwendenden Mobiltelefons bestätigt.

6. Im Falle von SMS-Premium- oder ähnlichen Diensten sollte von dem Dienstanbieter von Zeit zu Zeit eine kostenlose Nachricht versandt werden, um festzustellen, ob der Nutzer diesen Dienst weiter in Anspruch nehmen will. Im Falle eines Bankkontos kann dies zum Beispiel durch die Einführung eines Berechtigungsmerkmals bestätigt werden, das nur der wirkliche Nutzer kennt und auf das nur er Zugriff hat.

7. Einzelpersonen (Arbeitnehmer) sollten für das Abonnement oder die Registrierung von Diensten privater Natur, wie mailing-Listen, e-shops, soziale Netzwerke, etc. keine e-mail-Adressen verwenden, die Anderen zugewiesen werden könnten (z. B. geschäftliche e-mail-Adressen).

8. Eine Person, die eine permanente Email-Adresse haben möchte, sollte einen persönlichen Domain-Namen registrieren, der auch als Homepage, Weblog etc. genutzt werden kann. Allerdings erfordert eine persönliche Domain in der Regel eine jährliche Erneuerung, anderenfalls kann sie verloren gehen und an eine andere Person vergeben werden.

9. Arbeitgeber und andere Organisationen, die geschäftliche Email-Adressen verteilen, sollten den Mechanismus festlegen, der eingreift, wenn ein Mitarbeiter geht oder seine Funktion innerhalb des Unternehmens wechselt. Nachrichten an eine solche Adresse sollten zurückgesandt werden, oder es sollte eine automatisierte Nachricht verschickt werden, sodass der Absender weiß, dass die Adresse des Angestellten sich geändert hat oder nicht mehr besteht. Es wird empfohlen, Bezeichnungen für persönliche e-mail-Adressen nicht wiederzuverwenden, wenn diese bereits ehemaligen Beschäftigten zugewiesen waren.

46th meeting, 7th and 8th September 2009, Berlin

Working Paper on privacy risks in the re-use of email accounts and similar information society services

– Revised and updated at the 47th meeting, 15–16 April 2010, Granada, Spain –

Introduction

For many people, email has become the primary means of communication, superseding traditional mail for both domestic and business purposes. An email account which can identify an individual and can be used for personal communications is universally regarded by data protection and privacy authorities as constituting personal data.

An individual may have one or many email accounts, which may have been provided via a free or a paid-for service; an employee may also be permitted by his employer to use a business email address for personal purposes. Apparently "free" email accounts may be packaged in with information services such as broadband services and cable TV.

So what happens if an individual needs to change his email service provider?

The real-world analogy is with moving house. Normally, when someone moves house, they send out letters to all their business and personal contacts informing them of the new address. In addition, the person will normally arrange with the postal services for all of their mail to be redirected to their new address – not a simple matter as nowadays there may be many postal delivery services involved. The 'backstop' is to give the new occupants re-address labels to use for any residual mail that arrives.

If we translate this real-world analogy into cyberspace then we need to consider any information society service that involves identifying an individual by name. This can include the increasingly popular social networking services and cyber-trading accounts which use an email address for validation purposes and to which electronically delivered goods and invoices, etc. may be sent. The problem may also manifest itself in the case of SMS messaging associated with mobile phones.

Changing an email address or information society service account

If an email address or cyber-account is terminated, the possibility arises that a new user may be able to reuse the username and then inherit its history. This possibil-

ity is fairly remote in the case of free "email-for-life" services (such as gmail or hotmail), as such service providers would rarely reallocate ceased accounts.

Unless the individual has paid for a personal domain, the likelihood is that the email domain name will be associated with the service provider and not be transferrable from one provider to another.

By way of example, consider someone with a common name, such as Joe Doe, who lives in Portugal, uses gmail, subscribes to a cable TV channel and works for a company called Xpto; Joe may have a number of email accounts, such as **joedoe99@gmail.com**, **joedoe@cabletv.pt**, or **joedoe@xpto.pt**. Additionally, he may have purchased or use a personal domain for his family, such as **doe.pt** and use the email address **joe@doe.pt**.

If he wishes to cease his gmail account, he can be fairly confident that the account **joedoe99@gmail.com** will not be reallocated, but if he terminates his cable TV subscription or moves his employment, then he may discover that he is no longer able to access his email from the addresses **joedoe@cabletv.pt** or **joedoe@xpto.pt**.

On the other hand, the personal domain **doe.pt** should be readily portable from one service provider to another, provided that he or his family continues to pay for it.

However, if his former cable TV supplier has a new customer or his former employer has a new employee also called Joe Doe, they may decide to reallocate his previous email address to this new person. In such a case, the new 'owner' of the email address may well inherit email messages and personal information intended for its former owner.

Similarly, any new owner of a reallocated personal domain where the payment has lapsed may inherit email traffic intended for the former owner.

Possible adverse consequences

There could be several adverse consequences:

- if the user did not cancel newsletter subscriptions or inform all his contacts of the change to his address, the new owner of the address will start to receive information intended for the former owner, leading to a potential disclosure of personal data;

- If the user uses the "forgot-password option" of a third party where he registered under the old mail-address, the new owner would receive his username and personal password to use the site;

- in the case of leaving employment, the new employee could receive personal messages intended for the former employee as well as business email intended for whoever replaced the former employee;

- in the case of terminating a contract with an ISP, the new costumer could impersonate, on purpose or by coincidence, the former owner of the e-mail address.

Similar considerations apply to other Information Society services such as instant messaging, VoIP internet phone services and social networking services, especially where email addresses may additionally be used for authentication. If a subscriber wishes to cease a service, then the new subscriber may receive messages intended for the former subscriber, or more seriously, attempt to impersonate the former subscriber.

Whilst MNP, mobile number portability, may reduce the possibility of this problem occurring with SMS messages associated with mobile phones, the opportunity for MNP may not always be available (e.g. in case of lack of awareness, moving to a different country, death of a subscriber, or with some forms of anonymous or pay-as-you go services), so again there is the possibility that someone else may inherit a recently used mobile number and the SMS heritage that is associated with it.

This is particularly problematic as SMS messaging is commonly used in particularly confidential areas such as online banking, e-ticketing, etc.

Although the portability of mobile telephone numbers has helped to address these problems, the subscriber may feel that he needs to keep an e-mail address or mobile number with a certain ISP or mobile service provider just in order to protect his privacy and personal security.

Recommendations

The Working Group has previously considered privacy and security aspects of telecommunications services[1], internet services[2] and social network services[3].

The Working Group considers that a provider of Information Society Services (referred to below as “the ISP”) should provide facilities that would enable a sub-

[1] Common Position on the incorporation of telecommunications-specific principles in multi-lateral privacy agreements (Berlin 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

[2] Working Paper on privacy and security in Internet telephony (Berlin 5/6.09.2006); http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_en.pdf?1201702629

[3] Report and Guidance on Privacy in Social Network Services – “Rome Memorandum” (Rome 3/4.04.2008); http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

scriber to a service to mitigate any damaging consequences of terminating their contract, and makes the following recommendations:

1. The ISP should impose a "suspense period" of at least three months before anyone could take over the e-mail address, personal domain name or telephone number of a former subscriber.

2. The ISP should provide the subscriber with an opportunity, for the duration of the suspense period, to have messages sent to a suspended e-mail address or telephone number to be rerouted or auto-responded with a suitable message.

3. The ISP should provide a warning text alerting subscribers of the risk of losing their email address when terminating a contract and the potential consequences of data disclosure.

4. The ISP could offer a feature such as a roaming folder, where the subscriber could archive the login information that is used for web services where he registered using his e-mail-address or mobile telephone number. If the account is cancelled or contract not renewed then the user could transfer this folder to another service or at least would have a list of all third party services connected to this email-address or mobile number and could change the email-address or mobile number there. This would require that the user keeps such information up to date.

5. Services which use SMS authentication (e.g. in online banking) should display the number to which the message was sent. If the service does not receive any feedback from the user to continue a transaction within a certain time limit, the mobile number should be considered compromised and suspended until the owner of the account confirms once again the number of the mobile phone to be used.

6. In case of premium services via SMS or similar services, a time-to-time message, free of charge, should be sent by the service provider to verify if the user still wants to continue subscribing the service. In a case of bank account, it can be confirmed by the introduction of part of a credential that only the real-user knows and has access to, for example.

7. Individuals (Employees) should avoid using email addresses which can be subject to reallocation (e.g. business email address) for subscription and/or registration to services of personal interest, e.g. mailing lists, e-shops, social networking services, etc.

8. An individual wishing to have a permanent email address should register a personal domain name, which can be used as homepage, weblog, etc. However, a

personal domain normally requires renewing annually otherwise it may be lost and reassigned to another individual.

9. Employers and other organizations which allocate business related e-mail addresses should clarify the procedure to be used when an employee leaves or changes his role within the organization. Messages directed to such an address should be redirected or auto-responded such that the sender is aware that the employee's address may have changed or have been discontinued. It is recommended not to re-use identifiers for personal e-mail-addresses of future employees, when they had already been assigned previously to former employees.

2010

47. Sitzung, 15. und 16. April 2010, Granada, Spanien

Die „Granada Charta" des Datenschutzes in einer digitalen Welt[1]

Die internationale Gemeinschaft hat sich seit langem mit Fragen des Informationszeitalters befasst. Im Laufe der letzten Jahrzehnte wurden die folgenden internationalen Dokumente verabschiedet:[2]

– Europäische Menschenrechtskonvention vom 4. November 1950

– OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten vom 23. September 1980

– Übereinkommen 108 des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten

[1] Aufgrund von Unvereinbarkeit mit dem nationalen Recht in Schweden hat sich die schwedische Delegation bei der Verabschiedung dieses Arbeitspapiers der Stimme enthalten.

[2] Außerdem wurden die folgenden Empfehlungen und Entschließungen veröffentlicht: International Working Group on Data Protection in Telecommunications, Zehn Gebote zum Schutz der Privatsphäre im Internet, 13.–14. September 2000, Berlin; International Working Group on Data Protection in Telecommunications, Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum", 3.-4. März 2008, Rom, Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, Entschließung zum Datenschutz in sozialen Netzwerkdiensten, Straßburg, 17. Oktober 2008, Internationale Datenschutzkonferenz, Entschließung zum Datenschutz bei Suchmaschinen, London, 2.–3. November 2006

– Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, angenommen durch Entschließung der Generalversammlung vom 14. Dezember 1990

– Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

– Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000

– Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

– APEC Leitprinzipien zum Schutz der Privatsphäre von November 2004

– Gemeinsamer Vorschlag zur Erstellung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten[3]

In einer durch Interaktivität geprägten Welt sind die Einzelnen nicht mehr bloß Nutzer, sondern Netzbürger mit unveräußerlichen Rechten. Als solche sind sie aber auch verantwortlich für Inhalte, die sie über sich und andere veröffentlichen. Der Datenschutz und der Schutz der Privatsphäre sind äußerst wichtige Bestandteile einer demokratischen Informationsgesellschaft. Die folgenden Grundsätze sollen Teilnehmern, Anbietern und öffentlichen Stellen helfen, einen freien Informationsfluss zu gewährleisten und dabei die Würde, die Privatsphäre und den Schutz der Daten der Einzelnen zu respektieren. Es ist offensichtlich, dass zwischen diesen Grundsätzen und anderen wichtigen Werten wie freie Meinungsäußerung, Sicherheit und Eigentumsrechten Spannungen auftreten können. In jedem Einzelfall muss jede Maßnahme zur Durchsetzung dieser konkurrierenden Ziele mit dem Recht auf Datenschutz und der Privatsphäre in Ausgleich gebracht werden.

Teilnehmer und Nutzer der Kommunikationsdienste sollten

1. mit Sorgfalt vorgehen, wenn sie ihre eigenen personenbezogenen Daten oder Daten anderer veröffentlichen und sich dabei bewusst sein, dass die Löschung von Daten aus dem Internet weitaus größere Schwierigkeiten bereitet als deren Veröffentlichung

[3] Verabschiedet von der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre am 5. November 2009; http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2009-Madrid-InternationaleStandards.pdf?__blob=publicationFile

2. alle notwendigen Anstrengungen unternehmen – wie beispielsweise das Einholen einer vorherigen Einwilligung – um die Rechte einer jeden Person vor der Preisgabe oder Veröffentlichung ihrer Daten zu gewährleisten und ihre oder seine Entscheidung zu respektieren, eine gegebene Einwilligung zurückzuziehen

3. das grundlegende Recht haben, dass die rechtmäßige Nutzung von Kommunikationsdiensten privat und unbeobachtet bleibt und dass sie nicht abgehört und überwacht wird

4. die Möglichkeit haben, die Dienste anonym oder unter einem Pseudonym zu nutzen. Ihnen sollte auch die Möglichkeit eingeräumt werden, verschlüsselte Kommunikationen zu nutzen, insbesondere bei der An- und Abmeldung

5. das Recht haben, den Umfang personenbezogener Informationen zu kontrollieren, und auch die Nutzung dieser personenbezogenen Informationen

6. das Recht haben, über jede geplante Verarbeitung oder sekundäre Nutzung ihrer personenbezogenen Daten informiert zu werden. Ferner muss Ihnen die Möglichkeit eingeräumt werden, ihre ausdrückliche Einwilligung zu geben (opt-in) und ihre Einwilligung für alle derartigen vorgeschlagenen Offenlegungen oder sekundäre Nutzungen nachträglich zurückzuziehen (opt-out)

7. das Recht haben, bezüglich der Sammlung und Nutzung aller Daten über die Nutzung von Dienstleistungen ihre Einwilligung zu erteilen und diese auch nachträglich zurückzuziehen

Anbieter von Informations- und Kommunikationsdiensten sollten

1. sicherstellen, dass Nutzer von Kommunikationsdienstleistungen mit Einrichtungen ausgestattet sind, die den oben aufgezeigten Anforderungen in Bezug auf die Nutzung gerecht werden

2. gewährleisten, dass diese Einrichtungen leicht zu nutzen sind und dass sie im Nutzerhandbuch gut beschrieben werden

3. alle Anfragen von Einzelnen zu Informationen, die über diese verarbeitet und an wen diese übermittelt werden, unverzüglich und sorgfältig beantworten. Außerdem sollen die Anbieter die Nutzer mit elektronischen Hilfsmitteln ausstatten, wie zum Beispiel einem Online-Zugang zu den sie betreffenden personenbezogenen Daten

4. sicherstellen, dass alle über die Nutzer gesammelten Informationen das für eine Dienstleistung notwendige Minimum darstellen und dass dieses

Minimum an Daten nicht länger als nötig für den zu leistenden Dienst gespeichert wird

5. spezielle Sicherheitsvorkehrungen zum Schutz sensibler Daten einrichten, wie zum Beispiel Verkehrsdaten und Ortungsdaten

6. das Fernmeldegeheimnis garantieren

7. angemessene technische und organisatorische Maßnahmen zur Wahrung der Sicherheit ihrer Dienste treffen

8. Teilnehmer oder registrierte Nutzer von Kommunikationsdienstleistungen im Falle eines besonderen Risikos eines Sicherheitsverstoßes, über derartige Sicherheitsvorfälle und über alle möglichen Abhilfemaßnahmen informieren.

Öffentliche Stellen[4] sollten

1. bezüglich der Verarbeitung aller personenbezogener Daten offen und transparent sein

2. von jeglicher Beobachtung, dem Abhören oder der Überwachung der Kommunikation absehen, solange dies nicht für Strafverfolgungszwecke unbedingt notwendig ist, gestützt auf eine spezifische Rechtsrundlage

3. gewährleisten, dass Einzelpersonen aller Generationen und jeglichen Bildungsstandes in der Lage sind, Zugang zu den notwendigen Kenntnissen zu erlangen, um vollständig am digitalen Kommunikationszeitalter teilnehmen zu können

4. sicherstellen, dass jeder, der nicht in der Lage ist, Mittel der elektronischen Information und Kommunikation zu nutzen oder dies nicht wünscht, die Möglichkeit hat, ohne unangemessene Nachteile Zugang zu öffentlichen Dienstleistungen hat

5. die Rechte der Nutzer und das Recht auf Datenschutz und Schutz der Privatsphäre in interaktiven Diensten durchsetzen und den Nutzern effektive Rechtsmittel zu verschaffen.

[4] Einschließlich des Gesetzgebers, wo dies angemessen ist

47th meeting, 15th and 16th April 2010, Granada, Spain

The Granada Charter of Privacy in a Digital World[1]

The international community has been dealing with questions of the information age for a long time. In the course of recent decades the following international documents have been adopted[2]:

– European Convention on Human Rights of 4 November 1950

– OECD Guidelines on the protection of privacy and transborder flows of personal data of 23 September 1980

– Council of Europe Convention No. 108 of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data

– United Nations Guidelines for the regulation of computerised personal data files, adopted by the General Assembly Resolution 45/90 of 14 December 1990

– European Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

– Charter of Fundamental Rights of the European Union of 7 December 2000

– European Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

– APEC privacy framework of November 2004

– Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data of 5 November 2009[3]

---

[1] Due to incompatibilities with the national legal situation in Sweden the Swedish Data Protection Board has abstained from the adoption of this working paper.

[2] In addition the following guidelines and resolutions have been published: International Working Group on Data Protection in Telecommunications, Ten Commandments to protect Privacy in the Internet World, 13–14 September 2000, Berlin; International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services – "Rome Memorandum", 3–4 March 2008, Rome; International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy Protection in Social Network Services, Strasbourg, 17 October 2008; International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy Protection and Search Engines, London, 2–3 November 2006

[3] Adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2009; cf. http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf

In the interactive world individuals are no longer merely users, but they are also net citizens with inalienable rights. Moreover, they are also responsible for the contents they are publishing about themselves and others. Privacy and data protection are crucial elements of a democratic information society. The following principles should help users, providers and public authorities to facilitate a free flow of information whilst respecting the dignity, privacy and data protection of individuals. It is evident that tensions may occur between these principles and other important values such as freedom of expression, security and property rights. In each case every measure to enforce these competing objectives must be balanced with those of data protection and privacy.

Subscribers to and Users of Communications Services should

1. be careful when publicising personal data related to themselves or to other individuals and be aware that it is much more difficult to remove data from the Internet than to release it

2. undertake all appropriate efforts – for example obtain prior consent – to ensure the rights of any other person prior to the disclosure or publication of that person's information and to respect his or her decision to withdraw given consent

3. have the fundamental right to have their lawful use of communications services private, unobserved, not intercepted and not monitored

4. have the opportunity to use services anonymously or under a pseudonym and to use encrypted communications, especially when signing in and out

5. have the right to control the amount of personal information and the uses to which such personal information may be put

6. have the right to be informed as to any proposed processing or secondary uses of their personal data and – as appropriate – to give explicit consent (opt-in) and subsequently withdraw consent (opt-out) to all such proposed disclosures or secondary uses

7. have the right to opt-in to and subsequently opt-out of the collection and use of any data concerning their use of the services.

Information and Communications Service Providers should

1. ensure that users of communications services are provided with facilities which meet the requirements on use identified above

2. ensure that such facilities are easy to use and well described in user guidance

3. respond promptly and accurately to all requests from individuals for details about the information which is processed about them and to whom such information may be disclosed and provide them with electronic means such as online access to the personal data relating to them

4. ensure that any information collected about users is the minimum needed to provide a service and is not retained for longer than necessary for that service to be provided

5. set up specific safeguards to protect sensitive information such as traffic and location data

6. guarantee the secrecy of communications

7. implement appropriate technical and organisational measures to safeguard the security of their services

8. inform subscribers or registered users of communications services in any case where there is a particular risk of a security breach, of such a risk and any possible remedies, and when a privacy breach has actually occured.

Public Authorities[4] should

1. be open and transparent as to the processing of all personal information

2. refrain from any observation, interception or monitoring of communications unless it is strictly necessary for law enforcement purposes based on a specific legal basis

3. ensure that individuals of all generations and literacy are able to have access to the skills necessary to enable them to participate fully in the digital communications age

4. ensure that anyone who is not able or does not wish to participate in the use of electronic information and means of communication has the opportunity to access public services without disproportionate disadvantage

5. enforce user rights and the right of privacy and data protection in the use of interactive services and give the data subjects effective remedies.

[4] This includes, as appropriate, legislators

48. Sitzung, 6. und 7. September 2010, Berlin

Arbeitspapier zur Nutzung von Deep Packet Inspection zu Marketing-Zwecken

Deep Packet Inspection (DPI) ist eine Technologie, die die Untersuchung[1] des Headers und von Teilen des Inhalts von Datenpaketen, die über Netzwerke übertragen werden, in Echtzeit oder annähernder Echtzeit erlaubt.

Ein Internet-Paket oder „Datagramm" besteht gewöhnlich aus einem „Datagramm-Kopf" und einem „Datagramm-Daten-Bereich". Der Datagramm-Kopf ist der Teil des Pakets, der Informationen wie Quell- und Ziel- IP-Adresse enthält sowie andere Details, die notwendig sind, um das Paket dorthin zu leiten, wo es hin soll, während es das Netz durchquert. Der Datagramm-Daten-Bereich wird als „Nutzdaten" bezeichnet, weil er den Inhalt dessen bildet, was der Datagramm-Kopf (den „Umschlag") gewöhnlich zustellt. „Paketkopf" bezeichnet jegliche Information, die ein Dienstleister benötigt, um eine Telekommunikations-Nachricht zustellen zu können; die Nachricht selbst wird als der Inhalt oder die Nutzdaten dieser Telekommunikations-Nachricht bezeichnet.

Während DPI nicht als eine neue Technologie angesehen werden kann, da sie schon seit Jahren im Bereich der Intrusion Detection und -Prevention-Systeme wie auch in Firewall-Systemen eingesetzt wurde, wurden in jüngerer Zeit zusätzliche Nutzungen – ermöglicht durch leistungsfähigere Computer und effizientere Algorithmen – für das Netzverkehrsmanagement, zur Kontrolle der Verbreitung illegaler oder unerwünschter Inhalte – einschließlich urheberrechtsgeschützten Materials – und sogar für die Auslieferung benutzerspezifischer Werbung an Internetnutzer diskutiert und einzuführen begonnen.

Die Anwendung dieser Technologie kann die Privatsphäre von Internetnutzern Risiken aussetzen. Insbesondere können bestimmte Nutzungsarten von DPI-Technologien durch Internet-Zugangsdiensteanbieter zu erheblichen Beeinträchtigungen der Privatsphäre von Internetnutzern führen. Zugangsdiensteanbieter sind das „Eingangstor in die virtuelle Welt"; ihnen ist es technisch möglich, den Inhalt der gesamten Kommunikation eines Internetnutzers zu überwachen. Es ist

[1] In der Computertechnik werden Firewalls verwendet, um legitime Datenpakete für verschiedene Typen von Verbindungen zu unterscheiden. Nur Datenpakete, die einer vordefinierten Regel genügen, werden durch die Firewall durchgelassen, andere werden zurückgewiesen. Paketfilterung, oder „normale" Packet Inspection, arbeitet auf der Vermittlungsschicht (Schicht 3) und betrachtet nur den Header eines Pakets wie die Quell- und Ziel- IP-Adresse. Deep Packet Inspection (DPI) ist eine Firewall-Technologie, die auf der Anwendungsschicht (Schicht 7) des OSI-Modells arbeitet. DPI ermöglicht die Untersuchung des Inhalts von übertragenen Datenpaketen, wie der Kommunikation über HTTP und von Internet-Telefonie (VoIP)- Inhalten.

daher unerlässlich, dass Internet-Zugangsdiensteanbieter das Fernmeldegeheimnis respektieren, wie es in vielen Rechtsordnungen festgelegt ist. Darüber hinaus bieten Internet-Zugangsdiensteanbieter in vielen Fällen nicht nur Internetzugang an, sondern auch Internettelefonie und Zugang zu Medien, wie Kabelfernsehen. Anbieter solcher „triple-play"-Dienste können – technisch gesehen – ein noch detaillierteres Profil des Kommunikationsverhaltens ihrer Kunden erlangen. Mit dem Entstehen neuer und innovativer Dienste wie Telemedizin können darüber hinaus mehr und mehr besonders sensible personenbezogene Daten (wie Gesundheitsdaten) über Einrichtungen übertragen werden, die von Internet-Zugangsdiensteanbietern angeboten werden.

Die Arbeitsgruppe hat erhebliche Vorbehalte gegen den Einsatz von DPI für jegliche Zwecke außer der Gewährleistung der Sicherheit von Informationssystemen und -Netzen innerhalb einer Organisation[2], oder soweit es sonst durch das anwendbare Recht erlaubt oder gefordert wird.

Die Arbeitsgruppe insbesondere besorgt, dass jegliche zusätzliche Anwendung von DPI durch Internet-Zugangsdiensteanbieter und andere Internetdiensteanbieter in einer weiteren Erosion des Fernmeldegeheimnisses münden wird. Sie wird auch die Vertrauensbeziehung zwischen diesen Anbietern und ihren Kunden beschädigen.

Die Anwendung von DPI bei Internet-Zugangsdiensteanbietern kann in der Informationsgesellschaft auf das Äquivalent des Abhörens von Telefongesprächen hinauslaufen. Die Gruppe unterstreicht ihre Position, die bereits in früheren Veröffentlichungen niedergelegt ist, dass Netzwerk- und Diensteanbieter (einschließlich Internet-Zugangsdiensteanbieter) prinzipiell jegliche Inhalte einer Kommunikation nicht abhören oder stören dürfen, außer wo dies durch das anwendbare Recht ausdrücklich erlaubt oder gefordert wird[3] (informationelle Gewaltenteilung). Dies wird heutzutage auch unter der Überschrift „Netzneutralität" diskutiert.

Empfehlungen

Im Lichte des oben gesagten fordert die Arbeitsgruppe Internet-Zugangsdiensteanbieter auf, insbesondere die Nutzung von DPI-Technologie für zielgerichtete beziehungsweise verhaltensbasierte Werbung zu unterlassen.

---

[2] Vergleiche Arbeitspapier zu Intrusion Detection–Systemen (IDS) (Berlin, 02./03.09.2003); http://www.datenschutz-berlin.de/attachments/229/enum_de.pdf

[3] Vergleiche gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz – zehn Gebote zum Schutz der Privatheit im Internet (Berlin, 13./14.09.2000); http://www.datenschutz-berlin.de/attachments/215/tc_de.pdf

Zusätzlich fordert die Arbeitsgruppe die vermehrte Anwendung sicherer Ende-zu-Ende-Verschlüsslungsmechanismen. Das (optionale) Angebot solcher Technologien sollte gesetzlich vorgeschrieben werden wo dies nicht bereits der Fall ist, wenigstens für Anbieter, deren Dienste die Verarbeitung besonders sensitiver Daten beinhalten (z. B. Online-Banking, Nutzungen, die Kreditkarteninformationen beinhalten, Gesundheitsdaten, usw.) wie auch für Anbieter von Kommunikationsdiensten (wie E-Mail, Chat, Internettelefonie – VoIP, usw.)[4].

48th meeting, 6th and 7th September 2010, Berlin

Working Paper on the Use of Deep Packet Inspection for Marketing Purposes

Deep Packet Inspection (DPI) is a technology that automates the inspection[1], in real or near-real time, of the header and content portions of data packets being transmitted on networks.

An Internet packet or datagram is generally composed of a 'datagram header' and a 'datagram data area'. The datagram header is the portion of the packet that contains information such as source and destination IP address and other details necessary to get the packet where it needs to go as it traverses the network. The datagram data area is referred to as the 'payload' because it is the content that the datagram header (the 'envelope') generally delivers. The packet header refers to any information a carrier requires to convey its telecommunications message, and the message itself is referred to as the content or payload of that telecommunications message.

While DPI cannot be considered a new technology, having been used for years in intrusion detection and prevention systems as well as in firewall systems,

[4] Vgl. Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet (Budapest-Berlin Memorandum) (Berlin, 19.11.1996), Punkt 7 auf Seite 2; http://www.datenschutz-berlin.de/attachments/137/bbmen_de.pdf

[1] In computing, a firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a predefined rule will be allowed by the firewall, others will be rejected. Packet filters, or normal packet inspection, operates at the network layer (layer-3) and looks only at the header part of a packet, such as source and destination IP address. Deep Packet Inspection (DPI) is a firewall technology that operates at the application level (layer-7) of the OSI model. DPI enables the inspection, of the content of data packets being transmitted, such as HTTP communication and VOIP payload.

additional uses – enabled by increased computing power and more efficient algorithms – for traffic management, control over the dissemination of illegal or unwanted content – including copyrighted material – and even for delivering targeted advertisements to Internet users have been discussed and started to be introduced more recently.

The application of this technology can put the privacy of Internet users at risk. In particular, certain uses of DPI technologies by Internet access providers can result in severe infringements of privacy of Internet users. Access providers are the "gateway to the virtual world"; they are technically able to monitor the content of the entire communication of an Internet user. It is therefore essential that Internet access providers respect telecommunications secrecy, as laid down in the legal frameworks of many jurisdictions. In addition, Internet access providers in many cases not only offer Internet access, but also voice telephony services, as well as access to media, such as cable television. Providers of such "triple play"-services can – technically speaking – gain an even more detailed profile of the communications behaviour of their customers. Furthermore, with the advent of new and innovative services like telemedicine, more and more personal data of a particularly sensitive nature (such as health data) may be transmitted through facilities offered by Internet access providers.

The Working Group has strong reservations about the application of DPI for any purposes other than maintaining the security of information systems and networks within an organisation[2], or as otherwise allowed or required by applicable legislation.

Specifically, the Working Group is concerned that any additional applications of DPI by Internet access providers and other ISPs will result in the further erosion of telecommunications secrecy. It will also damage the trust relation between these providers and their customers.

The application of DPI by Internet access providers can amount to the information society equivalent to wiretapping telephone conversations. The Group reinforces its position already laid down in earlier publications that, as a matter of principle, Network and Service Providers (including Internet access providers) must not intercept or interfere with any content of communications except where explicitly allowed or required by applicable legislation[3] (informational separation of powers). Nowadays this is also discussed under the heading of "network neutrality".

---

[2] Cf. Working Paper on Intrusion Detection systems (IDS) (Berlin, 02./03.09.2003); http://www.datenschutz-berlin.de/attachments/203/ids_en.pdf?1177660658

[3] Cf. Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

Recommendations

In the light of the above, the Working Group calls upon Internet access providers to specifically refrain from using DPI technology for targeted/behavioural advertising.

In addition, the Working Group calls for more widespread application of secure end-to-end encryption mechanisms. The (optional) provision of such technologies should be mandated by law where this is not already the case, at least for content providers offering services that involve the processing of sensitive data (e.g. online banking, uses involving credit card information, health data, etc.) as well as providers of communications services (like e-mail, chat, VoIP, etc.)[4].

Arbeitspapier

„Mobile Verarbeitung personenbezogener Daten und Datensicherheit“

Hintergrund

Im April 2004 hat die Arbeitsgruppe ein Arbeitspapier über potentielle Risiken für die Privatsphäre in Verbindung mit drahtlosen Computernetzwerken *(engl. wireless networks)* angenommen.[1]

Seither wird durch die stark steigende Verbreitung und Vielfalt von mobilen Geräten, wie zum Beispiel Mobiltelefonen, Smartphones, Laptops und PDA's, einhergehend mit der ständigen Verfügbarkeit von öffentlichen Kommunikationsnetzen eine Verarbeitung jeglicher Art von vertraulichen und persönlichen Daten auf potenziell unsicheren Geräten in potenziell unsicheren öffentlichen Umgebungen immer einfacher.

Der Einsatz mobiler Geräte ist nicht ausschliesslich auf die Pflege von Kontaktdaten und die Bearbeitung von Kalendereinträgen beschränkt. Vielmehr ist ein Zugriff auf vertrauliche und persönliche Informationen in Unternehmens-Datenbeständen oder die Nutzung von Cloud-Computing-Diensten bequem möglich.

Die stetig steigenden Speicherkapazitäten der mobilen Geräte und die immer schneller werdenden drahtlosen Netzwerke erlauben eine mobile Datenverarbei-

[4] Cf. Report and Guidance on Data Protection and Privacy on the Internet (Budapest-Berlin Memorandum) (Berlin, 19.11.1996), Item 7 on page 2; http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf?1200577389

[1] http://www.datenschutz-berlin.de/attachments/196/1_de.pdf?1215693415

tung in einer Art und Weise, die in der Vergangenheit nur in festen und sichereren Umgebungen möglich war. Die verstärkte Integration mobiler Anwendungen in herkömmliche betriebliche IT-Infrastrukturen und Prozesse hat zur Folge, dass zunehmend vertrauliche, persönliche sowie geschäftskritische Daten nicht nur in zentralen Systemen abgespeichert sind, sondern auf den mobilen Geräten bearbeitet werden. Dies kann sich unmittelbar auf die Integrität, Vertraulichkeit und Sicherheit der Daten auswirken.

Zudem werden mobile Geräte vermehrt zur Archivierung und temporären Speicherung von Daten genutzt, was die Risiken von Datenverlust oder Veröffentlichung mit sich bringt.

Datenschutz und Datensicherheitsrisiken

Naturgemäss besitzen mobile Geräte eine kleine Bauform und ein geringes Gewicht. Die grössten Gefahren für die Datensicherheit liegen in der Manipulation, dem Verlust und dem Diebstahl der Daten. Zur Erkennung einer Datenmanipulation existieren geeignete Mechanismen zur Sicherung der Datenintegrität. Während der Verlust von Daten sofort erkennbar ist, wird ein Datendiebstahl oftmals erst dann bemerkt, wenn die Daten selbst oder das Ergebnis einer Bearbeitung an einem anderen Ort wieder auftauchen.

Es ergeben sich durch den Einsatz mobiler Geräte eine Reihe von spezifischen Risiken:

- Verbindungen zu öffentlichen Netzwerkzugängen (z. B. offene Internetzugänge in Restaurants, Hotels, Internetcafes, usw.), ungeachtet der Anschlussart (z. B. Verbindung mit Netzwerkkabel oder Wireless LAN), alleinig mit einem nicht vertrauenswürdigen Netzwerk. Zumindest die Verbindungsdaten oder unter Umständen sogar die Inhaltsdaten können abgehört und mitgelesen werden. Das Abhören vertraulicher Informationen in der Kommunikation ist nicht nur für den Betreiber des Netzwerks, sondern, bei nicht ausreichenden Sicherheitsvorkehrungen im entsprechenden Netzwerksegment, von jedem Netzwerkanschluss aus möglich.
- Bei der Verwendung offener unverschlüsselter drahtloser Netzwerkzugänge, sogar bei sonst sicherer Netzwerkverbindung, kann die Nutzerkommunikation unbemerkt ausspioniert werden.
- Durch die laufende unbemerkte Auswertung von Standortdaten eines mobilen Geräts, z. B. durch im Hintergrund laufender standortbezogener Dienste *(Location Based Services – LBS)*, kann ein Bewegungsprofil des Nutzers erstellt werden.[2]

[2] Gemeinsamer Standpunkt der IWGDPT zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, http://www.datenschutz-berlin.de/attachments/192/local_neu-de.pdf

- Angriffe auf die Verfügbarkeit von mobilen Geräten sind unter Umständen leichter durchführbar (z. B. Störsignale auf den entsprechenden Frequenzbändern) als vergleichbare Attacken auf Arbeitsplatzrechner.

- Durch die Nutzung von Kurzstreckenfunkverbindungen wie z. B. Bluetooth, die es einem Angreifer unter Umständen ermöglichen, die Kontrolle eines ungeschützten Geräts zu übernehmen.

- Zudem ergeben sich Risiken im Zusammenhang mit der Speicherung und der direkten Datenverarbeitung auf mobilen Geräten:

- Mobile Geräte werden oft vom Anbieter mit zahlreichen zusätzlichen Anwendungen zur Datenverarbeitung ausgeliefert. Von einem seriösen Anbieter ist zu erwarten, dass dieser entdeckte Mängel und Verwundbarkeiten vor der Veröffentlichung der Software behebt. Allerdings können andere Firmen und Privatpersonen durch teilweise offene und dokumentierte Programmierschnittstellen und Entwicklungsumgebungen Software (so genannte „Apps“) für mobile Geräte entwickeln und über das Internet einfach und kostengünstig verbreiten. Durch die Installation solcher Fremdanwendungen von Dritt-Anbietern steigt das Risiko der Infektion durch Schadsoftware bzw. der Datenbeschädigung durch unsichere Applikationen. Die Stabilität des gesamten Systems kann durch die nachträgliche Installation von nicht beglaubigter (zertifizierter) Drittsoftware beeinträchtigt werden.[3]

- Durch die Entwicklung einheitlicher Betriebssysteme und Standards für mobile Geräte wird zwar die Softwareentwicklung vereinfacht. Diese Standardisierung kann aber bei Verwundbarkeiten zu einem erhöhten Risiko der Verbreitung von Schadsoftware führen, wie es bereits in der Welt des „personal computing“ sichtbar ist. Allerdings ermöglichen einheitliche Betriebssysteme die Implementierung einheitlicher Sicherheitsmaßnahmen.

- „Push-Dienst“ oder „Server-Push-Dienst“ beschreibt eine meist internetbasierte Methode der Inhaltsverbreitung. Dabei werden Informationen von einem zentralen Server direkt an das mobile Geräte exportiert und dort unmittelbar verarbeitet. Durch eine ungeprüfte Verarbeitung der eingehenden Nachrichten entstehen Risiken, die heute aus dem Bereich der Email-Verarbeitung auf Arbeitsplatzrechnern bereits bekannt sind (z. B. Schadsoftware in Anhängen, Ausnutzung von Schwachstellen in der Verarbeitungssoftware, usw.).

Die Erfahrung zeigt, dass eine Balance zwischen der Implementierung von zu restriktiven und möglicherweise von den Nutzern daher nicht akzeptierten Sicherheitsvorgaben im Umgang mit mobilen Datenträgern sowie Geräten einerseits

[3] Im gegenständlichen Arbeitspapier bleiben sämtliche Aspekte der Privatsphäre im Zusammenhang mit Drittanbieter-Software unberücksichtigt.

und der Bereitstellung eines sicheren Umfelds mit ausreichendem Schutz der Daten andererseits gefunden werden muss.

Die bloße Verschlüsselung der Daten und sensitiver Informationen *ohne* die Anwendung begleitender Massnahmen und von Verhaltensstandards ist *kein* effektiver Weg, um jeglichen Risiken und Sicherheitsbedenken zu begegnen.

Empfehlungen

Basierend auf den oben angeführten Risiken richtet die Arbeitsgruppe folgende (vorläufige) Empfehlungen an Anbieter und Nutzer mobiler Endgeräte.

Anbieter

Die grundlegenden Sicherheitseinstellungen des mobilen Geräts sollten bei der Auslieferung das höchste Mass an Sicherheit berücksichtigen und im Einklang mit dem Zweck stehen, für den das Gerät vermarktet wird.

Ein oder mehrere Nutzerprofile mit konfigurierbar eingeschränkten Rechten sollte existieren, zusammen mit einem „Super-User“, der den Zugriff auf die Sicherheitseinstellungen für diese Nutzerprofile kontrollieren und einschränken kann.

Der Nutzer sollte in einfacher Weise über jegliche Änderung an den Sicherheitseinstellungen informiert werden. Dies könnte zum Beispiel bei der Aktualisierung von Systemsoftware (z. B. Firmware- oder Betriebssystem-Update) oder durch die Installation von zusätzlichen Anwendungen der Fall sein.

Das Handbuch sollte jedenfalls ein eigenes Kapitel zum Thema „Sicherheit“ und den „Sicherheitseinstellungen“ enthalten. Dabei sollte auf die Risiken der Benutzung mobiler Geräte eingegangen und dem Nutzer ein übersichtlicher und verständlicher Leitfaden zur sicheren Handhabung gegeben werden.

Eingebaute Hardwarekomponenten und Schnittstellen, die zur Erhebung und Übermittlung von Daten dienen (z. B. Kamera, GPS, Mikrofon, IrDA, Bluetooth, WLAN, usw.), sollten werksseitig deaktiviert sein; diese Schnittstellen sollte, abhängig von den Rechten des entsprechenden Nutzerprofils, für den Nutzer verfügbar sein, und bei Bedarf aktiviert werden können.

Bei Mobiltelefonen kann der unbefugte Zugriff auf die SIM-Karte durch eine PIN geschützt werden. Über eine entsprechende Sicherheitseinstellung sollte dieser Zugriffsschutz auf den Telefonspeicher ausgeweitet werden können. Ein Nutzer sollte eine Zeitspanne bestimmen können, nach der das Gerät bei Inaktivität das Display/Tastatur sperrt und erst wieder nach erneuter Eingabe der PIN oder eines frei wählbaren Passworts freigibt.

Zur Kommunikation

Ein Nutzer sollte gewarnt werden, wenn möglicherweise unsichere Kommunikationskanäle für die Datenübertragung genutzt werden.

Wenn ein mobiles Gerät den Kontakt zu einer sicheren WLAN-Verbindung verliert und sich anschliessend automatisch mit einem unsicheren WLAN Netzwerk verbindet, sollte eine Warnung an den Nutzer ausgegeben werden.

Es sollte für einen Nutzer einfach erkennbar sein, ob externe Kommunikationskanäle und Schnittstellen aktiv oder inaktiv sind. Zusätzliche Dienste, wie z. B. Schnittstellen für die Kommunikation, sollten auf einem mobilen Gerät durch den Nutzer einfach ein- und ausgeschaltet werden können.

Zur Speicherung und Datenverarbeitung

Bei der nachträglichen Installation oder dem Herunterladen von nicht beglaubigter (zertifizierter) Software eines Drittanbieters sollte ein entsprechender Warnhinweis an den Nutzer ausgegeben werden.

Ein Nutzer sollte vor dem Herunterladen und vor der Installation von Applikationen die Möglichkeit haben, insbesondere den Namen und die elektronische Signatur des Anbieters, die Nutzungsbedingungen, die zur Ausführung erforderlichen Zugriffsrechte auf Gerätehardware sowie bereits installierter Software, Hinweise zur Deinstallation als auch weitere sicherheitsrelevante Informationen und Warnhinweise in einfacher Weise und in einer selbst gewählten Sprache einzusehen.

Ein Nutzer sollte die Möglichkeit haben, den Zugriff jeder installierten Applikation auf die verfügbare Gerätehardware (z. B. Netzwerkkarte, Kamera, usw.) sowie auch auf gespeicherte Daten (z. B. auf den Kalender oder das Adressbuch) einzuschränken.

Es sollte für den Nutzer einfach nachvollziehbar sein, welche Daten im mobilen Gerät verschlüsselt und welche unverschlüsselt abgespeichert werden.

Nutzer

Die Bewusstseinsbildung ist ein erster wichtiger Schritt zur Vorbeugung von Missbrauch, Datenverlust und Diebstahl. Die Nutzer sollten auf ihre Eigenverantwortung im Zusammenhang mit der Datensicherheit und Integrität hingewiesen werden. Unterstützend dazu folgende Empfehlungen:

Der Nutzer sollte nach einer Aktualisierung der Systemsoftware (z. B. Firmware-Update) die lokalen Sicherheitseinstellungen des mobilen Geräts überprüfen und wenn erforderlich auf die eigenen Bedürfnisse anpassen.

Bei Verwendung eines mobiles Geräts in einem öffentlichen Bereich, sollte der Nutzer alle Anstrengungen unternehmen, um sicherzustellen, dass der Bildschirm und die Tastatur durch Passanten oder Überwachungskameras eingesehen werden kann.

Bei der Nutzung mobiler Geräte eines Unternehmens, sind die durch die Fachabteilung erarbeiteten organisatorischen Massnahmen unbedingt einzuhalten. Technische Manipulationen und Änderungen an den Systemeinstellungen sollten unterlassen werden.

Zur Kommunikation

Öffentliche Internetzugänge sollten mit Vorsicht verwendet werden. Vertrauliche Informationen und Daten sollten nicht über unsichere Netzwerkverbindungen verarbeitet werden, wenn die Übertragung nicht ausreichend durch zusätzliche Sicherheitsmassnahmen, wie z. B. einen virtual private network (VPN)-Tunnel, geschützt ist.

Vor dem Austausch von *vertraulichen* Informationen sollte die Identität des Kommunikationspartners geprüft werden. Jede unbekannte Meldung oder Unregelmässigkeit im Betrieb sollte hinterfragt und im Zweifel ein Experte oder in einem Firmenumfeld die verantwortliche Stelle Informiert bzw. zu Rate gezogen werden.

Für den unmittelbaren Betrieb nicht benötigte Schnittstellen sollten über die Einstellungen des mobilen Geräts deaktiviert werden (z. B. Einrichtungen zur Datenübertragung mit Bluetooth, Infrarotsignalen (IrDA), drahtlosen Netzwerken (WLAN), usw.). Speziell standortbezogene Dienste (Location Based Services – LBS) sollten deaktiviert sein, wenn sie nicht unmittelbar genutzt werden.

Zur Speicherung und Datenverarbeitung

Vor der Installation von Fremdapplikationen sollte die Quelle genau geprüft werden. Signaturen und Herstellerangaben können das Risiko einer Infektion minimieren. Im Zweifel sollte von einer Installation abgesehen werden.

Der Zugriff der installierten Fremdapplikationen sollte auf die für den ordnungsgemässen Betrieb erforderlichen Daten eingeschränkt werden. So benötigt zum Beispiel nicht jede Anwendung den Zugriff auf das Adressbuch oder den Kalender des mobilen Geräts.

Working Paper on

Mobile processing of Personal Data and Security

Background

In April 2004, the Working Group adopted a Working Paper on the potential privacy risks associated with wireless networks.[1]

Since that time, due to the strongly increasing dissemination and diversity of mobile devices such as, for example, mobile phones, smart phones, laptops and PDAs, accompanied by the constant availability of public communication networks, data processing of all manner of confidential and personal data on potentially insecure devices in potentially insecure public environments is becoming increasingly easy.

The use of mobile devices is not solely limited to the maintenance of contact data and processing of calendar entries. Rather, it makes confidential and personal data in corporate databases or the use of cloud computing services easily accessible.

The constantly increasing storage capacities of mobile devices and the ever-increasing speed of wireless networks allow mobile data processing in a way that was only possible in fixed and more secure environments in the past. The increased integration of mobile applications in conventional company IT infrastructures and processes increasingly results in confidential, personal, as well as business critical data not just being stored in the central system, but also being processed on the mobile devices. This can have a direct impact on the integrity, confidentiality and security of the data.

Furthermore, mobile devices are being increasingly used for archiving and temporary storage of data, which entails risks of data loss or disclosure.

Data protection and data security risks

By their very nature, mobile devices are small in design and light in weight. The major risks for data security lie in the manipulation, loss and theft of data. In order to recognise data manipulation, suitable mechanisms for securing data integrity

[1] http://www.datenschutz-berlin.de/attachments/197/1_en.pdf?1215693444

exist. Whereas the loss of data is immediately recognisable, data theft often goes unnoticed until the data itself or a processing result reappears at a different location.

A series of specific risks result due to the use of mobile devices:

- Connection to public network access points (e.g. open Internet access points in restaurants, hotels, Internet cafes, etc.), irrespective of the type of connection (e.g. connection via network cable or Wireless LAN), solely due to the untrustworthy network. At the very least the connection data or, possibly, even the content data can be intercepted and tapped. The interception of confidential information in the communication is not only possible for the network operator, but also, in the event of insufficient security precautions in the relevant network segment, from every network connection.
- The use of open unencrypted wireless access, even in otherwise secure networks, enables communication between users to be spied upon unnoticed.
- The ongoing unnoticed evaluation of a mobile device's location data, e.g. by location based services (LBS) running in the background, allows a user movement profile to be created.[2]
- Attacks on the availability of mobile devices are, possibly, easier to implement (e.g. interference signals on the relevant frequency bands) than comparable attacks on workplace computers.
- Under certain circumstances, the use of short range communication, such as Bluetooth, can allow an attacker to gain control of an unprotected device.

Furthermore, risks often arise in connection with storage and direct data processing on mobile devices:

- Mobile devices often already come with numerous additional applications from the supplier. A reputable supplier would be expected to eliminate deficiencies and vulnerabilities discovered in the software before publication. However, partially open and documented programmer interfaces and development environments allow other companies and private persons to develop software (so-called "Apps") for mobile devices and disseminate them easily and inexpensively via the Internet. The installation of such external applications from third-party providers increases the risk of infection by malware or damage to data by insecure applications. The entire system's stability can be adversely affected by the retroactive installation of uncertified third-party software.[3]

[2] Common Position of the IWGDPT on Privacy and location information in mobile communications services, http://www.datenschutz-berlin.de/attachments/193/local_neu_en.pdf

[3] All privacy aspects regarding third-party software are not considered in the current Working Paper.

- The development of uniform operating systems and standards for mobile devices is indeed simplifying software development. But in the event of vulnerabilities, this uniformity can lead to an increased risk of malware dissemination, as is already evident in the personal computing world. However, uniform operating systems facilitate the implementation of uniform security measures.

- "Push service" or "server push service" describes a method of content dissemination that is usually Internet-based. In the process information is outsourced from a central server directly to the mobile device where it is immediately processed. An unchecked dissemination of the incoming messages generates risks, which are already known today from the field of e-mail processing on workplace computers (e.g. malware in attachments, exploitation of weak points in the processing software, etc.).

Experience shows that a balance needs to be found between the implementation of too restrictive security requirements in dealing with mobile data carriers as well as devices on one hand, which may then not be accepted by users, and the provision of a secure environment with sufficient data protection on the other hand.

The mere encryption of the data and sensitive information without employing accompanying measures and behavioural standards is *not* an effective way to counter any risks and security considerations.

Recommendations

Based on the above-cited risks the Working Group makes the following (preliminary) recommendations addressed to suppliers and users of mobile devices.

Suppliers

When delivered, the default security settings of the mobile device should implement the maximum security in line with the purpose for which the device is marketed.

One or more configurable user profile settings with limited privileges should exist, together with a super user who can control and limit access to the security settings for a user profile.

The user should be informed in a simple way about any change in the security settings. This could, for example, happen when updating system software (e.g. firmware or operating system update) or due to the installation of additional applications.

The manual should include a chapter dedicated solely to the topic of “security” and “security settings”. The latter should deal with the risks of the use of mobile devices and give the user a transparent and comprehensible guideline for secure handling.

Built-in hardware components and interfaces used for the collection and transmission of data (e.g. camera, GPS, microphone, IrDA, Bluetooth, WLAN, etc.) should be disabled by default; these interfaces should be available for the user to activate when needed, dependent on the privileges associated with the user profile.

In the case of mobile phones, a PIN on the SIM card can offer protection against unauthorised access. This access protection should be able to be extended to the telephone memory via an appropriate security setting. A user should be able to specify an interval of time after which the device blocks the inactive display/keyboard and only releases it again once the PIN or a freely selectable password is re-entered.

With regard to communication

A user should be warned when possibly insecure communication channels are being used for data transfer.

If the device loses contact with a secure WLAN and subsequently automatically re-connects to an insecure WLAN, a warning should be issued to the user.

A user should be able to easily recognise whether external communication channels and interfaces are active or inactive. Additional services on a mobile device, such as e.g. interfaces for communication, should be easily switched on and off by the user.

With regard to storage and data processing

In the event of subsequent installation or downloading of untested (uncertified) software from a third-party provider, a corresponding warning notice should be output to the user.

Before downloading and installing applications, a user should have the opportunity to inform himself in a simple way and in a self-selected language specifically about name and the electronic signature of the provider, the terms of use, access rights to hardware components and other pre-installed software necessary for running the application, directions for de-installing the application, and additional warning notices and other information relevant to security.

A user should have the option of restricting the access of every installed application to the available device hardware (e.g. network interface card, camera, etc.) as well as to the stored data (e.g. to the calendar or the address book).

The user should be able to easily understand which data in the mobile device are encrypted and which are unencrypted when saved.

User

The raising of awareness is a first important step towards preventing misuse, data loss and theft. The users' own responsibility in connection with data security and integrity should be pointed out to them. The following recommendations are meant as a guide:

Users should review the local security settings of the mobile device following any system software upgrade (e.g. firmware update) and, if necessary, adjust them to meet their own needs.

When using a mobile device in a public area, users should make every effort to ensure that the screen and keyboard of their device are not observed by passers-by or surveillance cameras.

When using a company's mobile devices, compliance with the organisational measures developed by the technical department is imperative. Technical manipulations and changes to system settings should be prohibited.

With regard to communication

Public Internet access points should be used with caution. Confidential information and data should not be processed via insecure network connections unless the transmission is adequately protected by additional security measures, e.g. a virtual private network (VPN) tunnel.

Before exchanging confidential information, the communication partner's identity should be checked. Every unknown message or inconsistency in the operation should be questioned and, in case of doubt, an expert, or the responsible office in a corporate environment, should be informed or consulted.

Interfaces not required for actual use should be deactivated via the mobile device settings (e.g. facilities for transmitting data via Bluetooth, infrared signals (IrDA), wireless networks (WLAN), etc.). Location based services specifically should be deactivated, if they are not actually being used.

With regard to storage and data processing

Before installing external applications, the source should be meticulously checked. Signatures and manufacturer's specifications can minimise the risk of an infection. In case of doubt, an installation should be abandoned.

Access from installed external applications should be restricted to the data required for orderly operation. Thus, for instance, not every application needs access to the address book or calendar of the mobile device.

2011

49. Sitzung, 4. und 5. April 2011, Montreal, Kanada

Arbeitspapier

Datenaufzeichnung in Fahrzeugen (Event Data Recording – EDR): Fragestellungen zu Datenschutz und zum Schutz der Privatsphäre für Regierungen und Hersteller

Hintergrund

1. Der rasante technologische Fortschritt in der Informationsgesellschaft, insbesondere im Bereich Intelligente Verkehrssysteme (IVS), hat eine zunehmende Verarbeitung personenbezogener Daten in Fahrzeugen (PKW und LKW) sowohl für private als auch für kommerzielle Zwecke zur Folge.

2. Die nahezu allgegenwärtige Internetanbindung und immer größere Bandbreiten ermöglichen eine permanente Vernetzung sogenannter „Smart Vehicles" (Intelligente Fahrzeuge) und somit den Zugriff auf angefallene Daten. Diese alarmierende technische Entwicklung führt zu einer Eingliederung intelligenter Fahrzeuge in das sog. „Internet of Things", das die Verknüpfung von physischen Objekten, also Sachen, mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur beschreibt.

3. Ohne geeignete Maßnahmen zum Schutz der Privatsphäre wird es weder Fahrern noch Passagieren solcher „Smart Vehicles“ möglich sein, die Verarbeitung ihrer Daten zu kontrollieren oder zu überwachen. Sie werden sich dieser Verarbeitung vielmehr gar nicht bewusst sein.

4. Ungeachtet der mannigfaltigen Erscheinungsformen technologischer Anwendungen in Fahrzeugen behandelt dieses Arbeitspapier ausschließlich die Aspekte der Datenaufzeichnung.

Datenaufzeichnung in Fahrzeugen (EDR): Definitionen und Fakten

5. Im Moment eines Unfalls oder sonstigen Schadenseintritts werden verschiedene, durch Sensoren erfasste Daten mittels eines in das Fahrzeug eingebauten Geräts, dem „Event Data Recorder“ (EDR) oder auch Unfalldatenspeicher, gespeichert. Diese Geräte verarbeiten die Daten typischerweise innerhalb eines begrenzten Zeitraums im Zusammenhang mit einem Schaden, Unfall oder sonstigen Störfall verarbeitet (unmittelbar vor, während und nach dem Ereignis).

6. Der EDR kann sowohl ab Werk als auch nachträglich in das Fahrzeug eingebaut werden. Die gespeicherten Daten können mittels spezieller, für Endverbraucher meistens nicht frei verkäuflicher Software heruntergeladen werden.

7. Die im Schadensfall gesammelten und registrierten Daten beziehen sich nicht ausschließlich auf technische Gegebenheiten des Fahrzeugs (wie etwa den Kraftstoffverbrauch oder die Funktionsfähigkeit des Airbags) und den Schadenszeitpunkt, sondern lassen darüber hinaus (direkt oder indirekt) Rückschlüsse auf das Fahrerverhalten zu (z. B. Bremsöldruck zu Beginn und Ende des Bremsvorgangs, Geschwindigkeit, Bremsverhalten, Motordrehzahl, Gaslast, Verwendung oder Nichtverwendung von Sicherheitsgurten).

8. Es handelt sich somit um personenbezogene Daten des Fahrers und ggf. auch der Passagiere (z. B. hinsichtlich der Daten über die Benutzung des Sicherheitsgurtes).

EDR in Verbindung mit anderen „On-Board-Systemen“

9. Im Rahmen vertraglicher Vereinbarungen mit Mobilfunkanbietern sind die EDRs mit den im Fahrzeug verbauten Kommunikationssystemen verbunden, die im Falle eines entsprechenden Vorfalls die relevanten Informationen an bestimmte Empfangsstationen übermitteln. Die Übermittlung erfolgt durch ein Unfallerkennungssystem (oder eingebautes Notrufsystem), das zu die-

sem Zweck automatisch oder auch manuell aktiviert wird. In den USA[1] und der EU[2] wurden bereits Initiativen ins Leben gerufen, die den Einbau dieser Systeme und die Einführung allgemeiner technischer Standards in den verschiedenen Transportsektoren befördern sollen.

10. Um mehr Beweismaterial zu einem Unfall zu erhalten, operieren EDRs vereinzelt auch mit eingebauten Videokameras (sog. Video Event Data Recorder – VEDR), wodurch nochmals erheblich mehr Informationen über das Verhalten des Fahrers sowie über an dem Unfall beteiligte Dritte gespeichert werden.

Personenbezogene Fahrerdaten Daten beim Einsatz von EDR

11. Personenbezogene Fahrerdaten, die mittels EDR bzw. VEDR insbesondere im Zusammenhang mit elektronischen Kommunikations- und Lokalisierungssystemen gesammelt wurden, lassen sich von einer stetig wachsenden Anzahl von Interessengruppen zu den verschiedensten Zwecken verwenden:

    a) Hersteller, Fahrer (ebenso wie andere, in Verkehrsunfälle verwickelte Personen), Eigentümer (z. B. Autovermieter oder Firmenflottenverwalter) und Versicherungsgesellschaften könnten die EDR-Daten nutzen, um bei Rechtsstreitigkeiten Zeugenaussagen zu überprüfen;

    b) Polizei und andere Behörden (z. B. könnte die für die Sicherheit des Straßenverkehrs zuständige Behörde die Informationen zur Vervollständigung der Beweislage bei einem Verkehrsunfall nutzen);

    c) Arbeitgeber, aus organisatorischen und Sicherheitsgründen;

    d) Versicherungsgesellschaften, zur Einteilung der Kunden in spezifische Tarifgruppen (z. B. nach der Fahrweise oder nach Regionen, in die gefahren wird);

    e) Forschung, zur Verbesserung der Verkehrsinfrastruktur;

---

[1] Die US National Highway Traffic Safety Administration (NHTSA) hat im August 2006 entschieden, dass Hersteller nicht verpflichtet sind, EDRs in Neufahrzeuge einzubauen. Dennoch verlangt die NHTSA von den Herstellern den Einbau von EDRs, um jedenfalls einen Mindestdatensatz speichern zu können. Dieser soll 15 Typen von Unfalldaten beinhalten, darunter: Geschwindigkeit vor dem Unfall, Gaslast, Bremsverhalten, Geschwindigkeitsveränderungen, Sicherheitsgurtnutzung, Status der Airbag-Kontrolllampe und die Airbagauslösungszeit. Die Hersteller müssen sich mit diesen Standards bis September 2012 einverstanden erklären. http://www.nhtsa.gov/EDR

[2] Zur „E-call Intiative" der Europäischen Union im Einzelnen: Mitteilung der Europäischen Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, eCAll: Time for Deployment, Brüssel, 21.8.2009, KOM(2009) 434 endg.; http://ec.europa.eu/information_society/activities/esafety/ecall/index_de.htm .

f) Werbe- und Marketingagenturen könnten auf Grundlage der Daten Verhaltensanalysen durchführen, um so spezifisch zugeschnittene Angebote zu platzieren;

g) andere Dienstleister (z. B. Pannenhilfe).

12. Die oben aufgeführten Entwicklungen erfordern besonders sorgfältige Überlegungen in Bezug auf den Datenschutz und die Persönlichkeitsrechte sowohl der Fahrer als auch aller potentiellen Passagiere. Ein angemessener Ausgleich mit anderen individuellen Rechten und Interessen und mit dem öffentlichen Interesse an der Sicherheit des Straßenverkehrs muss erreicht werden.

13. Die Europäische Kommission hat 2008 eine Mitteilung betreffend einen Aktionsplan[3] zum Thema Intelligente Verkehrssysteme veröffentlicht. Gleichzeitig hat die Kommission eine entsprechende Richtlinie vorgeschlagen, die kürzlich durch den Rat und das Europäische Parlament verabschiedet wurde[4]. Diese Richtlinie, die bis Februar 2012 durch die Mitgliedsstaaten umgesetzt werden muss, verlangt beim Einsatz intelligenter Verkehrssysteme die Verwendung anonymer Daten, soweit dies angemessen ist[5]. Der Datenschutz und ein verantwortungsvoller Umgang mit den gesammelten Informationen sind in dem Aktionsplan wie in der Richtlinie von zentraler Bedeutung, um das Ziel effizienterer, umweltfreundlicher und sichererer Mobilität im Fracht- und Passagierverkehr innerhalb der Europäischen Union zu erreichen.

14. Durch das Rahmenprogramm für Forschung und technologische Entwicklung in der Europäischen Union wurde eine Vielzahl von Forschungsprojekten aufgelegt, die inzwischen teilweise abgeschlossen sind oder immer noch andauern, um die Sicherheit auf den Straßen zu erhöhen[6]. In einigen Jurisdiktionen wurden Gesetzesvorschläge entwickelt[7], in anderen sogar bereits Gesetze verabschiedet, die (unter anderem) auf den Schutz der Privatsphäre des Fahrers im Zusammenhang mit dem Einsatz von EDR abzielen[8].[9]

---

[3] Aktionsplan zum Einsatz intelligenter Verkehrssysteme In Europa (COM(2008) 886).

[4] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, Abl. L 207/1, 2010.

[5] Art. 10 Abs. 3 der Richtlinie 2010/40/EU

[6] Vgl. Intelligent Car Brochure, p. 16 auf: http://ec.europa.eu/information_society/activities/intelligentcar/docs/right_column/intelligent_car_brochure.pdf .

[7] Vgl. für die bundesstaatliche Ebene den Vorstoß durch *The Motor Vehicle Safety Act of 2010 (H.R. 5381)*.

[8] Kalifornien war der erste Staat, der gesetzlich verfügt hat, dass die Hersteller ihren Kunden gegenüber den Einbau von EDRs oder „black boxes" offenbaren müssen. Zur Gesetzgebung in Bezug auf Privatsphäre im Zusammenhang mit Datenaufzeichnung in Fahrzeugen siehe die Website der National Conference of State Legilatures auf: http://www.ncsl.org. Detaillierte Informationen zum aktuellen Stand in Sachen Datenaufzeichnung in Fahrzeugen in den U.S.A. finden sich auf der Seite der National Highway Traffic Safety Administration (http://www.nhtsa.gov/EDR).

[9] Vgl. für die bundesstaatliche Ebene den Vorstoß durch *The Motor Vehicle Safety Act of 2010 (H.R. 5381)*.

15. Zeitgleich wird von Seiten der Datenschutzbeauftragten ein Anstieg der EDR-Verwendung zur Verwaltung von Fahrzeugflotten registriert.[10] Im Rahmen der europäischen E-call Initiative hat die Artikel 29-Datenschutzgruppe bereits eine Reihe von Empfehlungen unterbreitet[11].

16. Die anstehende umfassende Einführung dieser Systeme, die Komplexität der Materie sowie die absehbaren notwendigen Investitionen (möglicherweise auch in Hinsicht auf die Verkehrsinfrastruktur) bedingen die dringliche Notwendigkeit eines klaren Regelwerkes, dem gleichwohl eine ausführliche öffentliche Auseinandersetzung mit der Thematik vorausgehen sollte. Der Entwicklung und Ausgestaltung eines solchen Regelwerkes sollte der Gedanke innewohnen, den Datenschutz von vornherein in die Gesamtkonzeption einbeziehen, anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme beheben zu wollen[12].

17. Vor diesem Hintergrund

ruft die Arbeitsgruppe die Regierungen dazu auf,

a) in Zusammenarbeit mit den Datenschutzbeauftragten und den betreffenden Interessenvertretern aus Industrie und Wirtschaft, ein angemessenes gesetzgeberisches Regelwerk darzulegen, zu definieren bzw. zu bestätigen (damit die Verarbeitung personenbezogener Daten auf gesetzmäßige Weise erfolgt und Missbrauch der durch EDR und möglicherweise andere intelligente Technologien in Fahrzeugen gesammelten und/oder übermittelten Daten ausgeschlossen oder eingeschränkt wird,

b) die Umsetzung der erforderlichen technischen Standards zu fördern und zu unterstützen, und

empfiehlt:

I. Transparenz

Jedwede Verwendung von Daten, die durch EDRs (oder andere intelligente Technologien) entstanden sind, sollte für den Fahrzeugeigentümer sowie die jeweiligen

[10] Französische Datenschutzbehörde (CNIL), Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommendation relative à la mise en oeuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme public ou privé; Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en oeuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules; Italienische Datenschutzbehörde (Garante per la protezione dei dati personali) on Geolocation in Public Transportation and Passenger Security, 5 June 2008, http://www.garanteprivacy.it , doc. no. 1672796

[11] Artikel 29-Datenschutzgruppe, Working document on data protection and privacy implications in eCAll initiative, WP 125, http//ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_de.pdf

[12] Vgl. ISO/TR Technical Report 12859 on Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems.

Fahrzeugnutzer in vollem Umfang transparent sein. Die Nutzer sind in die Lage zu versetzen, sich auf einfachstem Wege ein vollständiges Bild über die Erhebung und Speicherung sowie den Zweck der Verwendung aller sie betreffenden persönlichen Informationen machen zu können.

Zu diesem Zweck sollten:

a) *Hersteller/Systemintegratoren* ihre Kunden sorgfältig über die Verarbeitung personenbezogener Daten einschließlich der Möglichkeiten der Fahrzeugpositionsbestimmung aufklären. In dem Fahrzeug sollte ein (schriftlicher oder stimmlicher) Hinweis erfolgen. Ausdrückliche und detaillierte Informationen sollten im Benutzerhandbuch vorhanden sein.

b) *Datenverarbeitende Stellen* (wie etwa Arbeitgeber, Versicherer, Autovermietungen etc.) die Nutzer vollständig über (i) den Zweck der Verarbeitung erhobener Daten; (ii) die Kategorie(n) zu verarbeitender personenbezogener Daten; (iii) die Empfänger bzw. die Kategorien der Empfänger der Daten; und (iv) ihre Zugriffsrechte informieren.

II. Einwilligung des Eigentümers

Jegliches zur Speicherung personenbezogener Daten fähiges Gerät sollte regelmäßig nur nach der freiwilligen Einwilligung des ausführlich informierten Eigentümers und nach ausdrücklichem Hinweis an den Nutzer aktiviert werden. Zwingend notwendige Einbauten, die geeignet sind, personenbezogene Daten zu speichern oder an Dritte zu übermitteln, bedürfen einer gesetzlichen Grundlage, aus der vorgesehene Zweck der Speicherung personenbezogener Daten eindeutig hervorgeht.

III. Datenqualität

Die Datenaufzeichnung sollte nur solche personenbezogene Daten umfassen, deren Verarbeitung im Verhältnis zu dem Zweck ihrer Verarbeitung erforderlich und angemessen ist. Der Nutzung anonymisierter Daten sollte der Vorzug gegeben werden, wo immer dies möglich ist.

Entscheidungen anlässlich besonderer Vorkommnisse in Zusammenhang mit dem Fahrzeug sollten nicht ausschließlich von den Informationen aus der Datenaufzeichnung abhängig gemacht werden. Zu Zwecken der Qualitätsanalyse sind die aufgezeichneten Daten durch ausgewiesene Sachverständige zu prüfen und sorgfältig unter Heranziehung weiterer Nachweise und Begleitumstände abzugleichen.

IV. Privacy by Design

Das Leitmotiv bei der Entwicklung und Einführung von Systemen zur Datenaufzeichnung in bzw. der Interaktion mit Fahrzeugen sollte es sein, den Datenschutz

und den Schutz der Privatsphäre von vornherein in die Gesamtkonzeption einzubeziehen. Derartige Systeme sollten darauf ausgerichtet sein, die Notwendigkeit der Verarbeitung personenbezogener Daten zu minimieren und zugleich einen potentiellen Missbrauch personenbezogener Daten zu verhindern.

V. Zugriff auf (personenbezogene) Daten

Vor einer Einführung ist das Augenmerk auf den Schutz der Privatsphäre zu richten und klar festzulegen, wer unter welchen Voraussetzungen (z. B. Richtervorbehalt) auf die aufgezeichneten personenbezogenen Daten zugreifen darf. Dies gilt insbesondere in Hinsicht auf solche personenbezogenen Daten, die nicht ausschließlich vom Fahrer stammen. Ihm selbst ist das freie und vollumfängliche Zugriffsrecht auf seine eigenen Daten grundsätzlich zuzuerkennen. Hinsichtlich aller anderen Personen, deren personenbezogene Daten aufgezeichnet werden könnten, sollten klare und zweckmäßige Methoden zur Wahrung und ggf. Durchsetzung ihrer Rechte bereitgestellt werden. Eine vorherige Folgenabschätzung in Bezug auf den Datenschutz und den Schutz der Privatsphäre ist ein nützliches Instrument für eine solche Analyse.

VI. Datensicherheit und -integrität

Standardisierte Sicherheitsmaßnahmen zur Vermeidung unrechtmäßigen Zugriffs, Verlustes oder rechtswidriger Veränderung der aufgezeichneten Daten müssen festgelegt und universell umgesetzt werden. Um das Risiko unerwünschter Datentransfers und anderer schwerwiegender Angriffe von außen zu verringern, sollten zusätzlich verlässliche Verschlüsselungstechniken und Authentifizierungssysteme verwendet werden. Für den Endverbraucher sollte klar erkennbar sein, dass die im Fahrzeug verbauten Systeme zur Datenaufzeichnung und -übermittlung diesen Standards vollauf gerecht werden. Im Zusammenhang untereinander vernetzter Systeme sind entsprechende Sicherheitsmaßnahmen sogar von noch größerer Bedeutung.

VII. Überwachung von Arbeitnehmern

Darüber hinaus sind gesetzliche Regelungen zum Schutz von Arbeitnehmern vor Überwachung durch den Arbeitgeber zu beachten und zu respektieren, wenn dieser Systeme installiert, die der Verhaltenskontrolle von Arbeitnehmern oder der Ortung der Fahrzeugposition dienen (z. B. Fahrtenschreiber oder Lokalisierungsdienste).

49th meeting, 4th and 5th April 2011, Montreal, Canada

Working Paper

Event Data Recorders (EDR) on Vehicles: Privacy and data protection issues for governments and manufacturers

Scope

1. The fast pace of technological developments in the Information Society (IS) and in Intelligent Transport Systems (ITS) in particular has increased the processing of personal data in vehicles (cars and trucks), both for private and for commercial purposes.

2. The almost universal availability of network access points together with large bandwidth capability now create the opportunity to connect those smart vehicles to the network and to provide access to the data produced. This emerging technological trend will make the smart vehicle one of the components of the so-called Internet of Things.

3. Without appropriate privacy and data protection safeguards, drivers as well as passengers of “smart vehicles” may not have the ability to control or at least monitor their data processing, and even be unaware that such processing is taking place.

4. Although technological applications in the automotive sector are diverse, this paper considers only those aspects related to the data of the event recorder (EDR).

EDR: Definitions and facts

5. In the event of a vehicle crash or accident, data obtained from sensors are recorded via an onboard device, generally called an "Event Data Recorder" (EDR). EDRs typically process data during a limited timeframe covering only the vehicle crash, accident or serious incident (immediately before, during and after the event).

6. The EDR can be introduced into the vehicle during the production process or added later (aftermarket EDR). The recorded data can be downloaded using computer software which is not always commercially available to end users.

7. The data collected and registered in case of an accident does not simply reflect the technical status of the vehicle (fuel consumption, airbag functionality) and the time of the crash, but they will also register and describe (directly or indirectly) in a dynamic way the driver's behaviour (e.g., brake oil pressure at the beginning and end of braking, vehicle speed, including during braking, engine speed, percentage throttle, use or not of safety belts).

8. They are, therefore, personal data related to the driver and, in some cases, passengers (e.g., the information concerning the use of seat belts).

EDR coupled with other on-board systems

9. Based on agreements with mobile service providers, EDRs are being linked to onboard communication systems which transmit the relevant information to a remote location when the event occurs. A collision notification system (or in-vehicle emergency call system) can therefore be activated automatically or manually and provide data to emergency services. Initiatives have been launched in the US[1] and in the EU[2] in order to promote the implementation of such systems and to enforce standards across the different transport sectors and applications.

10. In order to get more evidence of an accident, sometimes EDRs are also associated with onboard cameras (Video Event Data Recorder-VEDR) which significantly increases the information collected related to the driver's behaviour and to third parties involved in the accident.

Driver-related personal data and the use of EDR

11. Driver-related personal data collected and transmitted via EDR (and also via a VEDR), especially when associated with electronic communication and localisation systems, offer numerous possible uses to a growing number of stakeholders:

    c) manufacturers, drivers (as well as other individuals affected by car accidents), owners (e.g., in the car rental or fleet management sectors) and

[1] The US National Highway Traffic Safety Administration (NHTSA) in August 2006 ruled (49 CFR Part 563) that manufacturers were not required to install Event Data Recorders in new vehicles. The NHTSA however required manufacturers who install EDRs to include a minimum standard set of data to be recorded: at least 15 types of crash data including pre-crash speed, engine throttle, brake use, measured changes in forward velocity, driver safety belt use, airbag warning lamp status and airbag deployment times. Manufacturers have until September 2012 to comply with the standards defined by the NHTSA. http://www.nhtsa.gov/EDR

[2] The European Union *"E-call initiative"* is detailed in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, eCall: Time for Deployment, Brussels, 21.8.2009, COM(2009) 434 final; http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm.

insurance companies, could use EDR data as evidence in order to check the accuracy of witness statements in cases of litigation;

d) police and other enforcement authorities (e.g., authorities in charge of car safety could use the information to complement other sources of information related to a vehicle accident);

e) employers, for organisational or security reasons;

f) insurance companies, to cluster the consumers and offer particular tariffs (e.g. "pay as you drive" or even "pay where you drive");

g) researchers (particularly vehicle and road safety sectors could use these data in order to improve the design of road infrastructures);

h) marketing organisations which could fine tune consumer behaviour analysis based on EDR data and deliver highly tailored advertising, or

i) other organisations offering services (e.g., roadside assistance), based on an analysis of such data.

12. The above developments require a careful consideration of the rights to private life and data protection for drivers as well as for other potential passengers. An appropriate balance with other individual rights and interests, as well as with the public interest in the safety of the transport network, must be established.

13. In 2008, the European Commission issued a Communication describing an ITS action plan[3] for Europe together with a proposal for a directive recently adopted by the Council and the European Parliament[4]. This Directive, which will have to be implemented in Member States by February 2012, encourages the use of anonymous data where appropriate for the performance of Intelligent Transport Systems applications and services[5]. Data protection and liability figure among the priority areas of the action plan and the Directive which aim at supporting more efficient, environment-friendly, safer and more secure freight and passenger mobility within the European Union.

14. The Research and Technological Development Framework of the European Union has launched a large number of RTD projects which have been final-

[3] Action Plan for the Deployment of Intelligent Transport Systems (ITS) in Europe (COM(2008) 886)

[4] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transports and for interfaces with other modes of transport, OJ 2010, L 207/1.

[5] Art. 10(3) of Directive 2010/40/EU.

ised or are still being carried out with a view to enhancing road safety.[6] In some jurisdictions, laws have been proposed[7] or have already been adopted to address (*inter alia*) the drivers' privacy issue in the context of EDR[8].[9]

15. Simultaneously Data Protection Authorities are noticing the increasing introduction of EDR and other smart vehicle technologies to support vehicle fleet management.[10] In the case of the European *E-call* initiative, the Article 29 Working Party has already made a series of recommendations[11].

16. The timing of a large scale implementation of these tools, the complexity of the topic and the considerable investment needed (possibly also in road infrastructures) give urgency to a clear regulatory framework, although this should not occur without an extensive public debate. The principle of "*Privacy by Design*" should be inherent in the development and clarification of this framework[12].

17. Against this background, the Working Group

calls

on regulators, in co-operation with Data Protection Authorities and the relevant industry stakeholders, to

a) set forth, clarify or confirm urgently an appropriate legislative framework (in order to establish the lawfulness of the data processing and to prevent or mitigate unauthorised use of the personal data collected and/or transmitted by EDR and, possibly, other smart vehicle technologies); and

b) promote the adoption of the relevant technical standards

---

[6] See *Intelligent Car Brochure*, p. 16 at http://ec.europa.eu/information_society/activities/intelligentcar/docs/right_column/intelligent_car_brochure.pdf.

[7] See, at federal level, the attempt done with *The Motor Vehicle Safety Act of 2010* (H.R. 5381).

[8] California was the first state to enact such legislation requiring manufacturers to disclose to customers whether event data recorders or *"black boxes"* are installed in vehicles. For privacy legislation related to Event Data Recorders ("Black Boxes") in Vehicles search the National Conference of State Legislatures website at http://www.ncsl.org. More detailed information on the state of the play regarding EDR in the U.S.A. can be found at the National Highway Traffic Safety Administration website (http://www.nhtsa.gov/EDR).

[9] See, at federal level, the attempt done with *The Motor Vehicle Safety Act of 2010* (H.R. 5381).

[10] *French DPA (CNIL), Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme public ou privé; Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules;* Italian DPA (Garante per la protezione dei dati personali) on Geolocation in Public Transportation and Passenger Security, *5th of June 2008, in* http://www.garanteprivacy.it*, doc. no. 1672796.*

[11] Article 29 Working Party, *Working document on data protection and privacy implications in eCall initiative*, WP 125, at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

[12] See ISO/TR Technical Report 12859 on Intelligent transport systems – System architecture – Privacy aspects in ITS standards and systems

recommends

I. Transparency

The data processing carried out through EDRs (and other smart technologies) in vehicles should be *completely transparent* to the vehicle's owner and user(s). Users should be put in a position to easily understand what items of personal information concerning them are collected and stored, as well for what purposes they are sought.

To this end:

a) *manufacturers/integrators* should make customers aware of the processing of personal data in the vehicle including any ability to locate the vehicle's position. A notice (written or voice) should be present in the vehicle. Clear and detailed information shall be provided via the owner's manual;

b) *data controllers* (such as employers, insurers, car rental companies, etc.) should fully inform the users regarding (i) the purpose(s) of the processing for which the data are collected; (ii) the category(ies) of personal data processed; (iii) the recipients or categories of recipients of the data; and (iv) their access rights

II. Owner's consent

As a rule, devices capable of storing personal data onboard should only be activated with the free and informed consent of the owner and after the user(s) have been informed. Mandatory installation of onboard devices capable of storing and communicating personal data to third parties requires an appropriate legislative basis that clearly identifies the envisaged purpose(s) of the recorded personal data.

III. Data quality

EDRs should only store personal data which are adequate, relevant and not excessive in relation to the purpose(s) for which they are processed. The use of anonymised data should be preferred wherever possible.

Decisions following an event relating to the vehicle should not be taken solely on the basis of information gathered through an EDR. In order to better analyse their quality, the data collected must be interpreted by certified experts and carefully evaluated along with all other relevant evidence and circumstances.

IV. Privacy by Design

Privacy by Design should be the guiding principle of any development and implementation of EDRs and other similar technological device built into a vehicle (or interacting with a vehicle). Such systems should therefore be designed to minimise the need for processing personal data and to prevent the potential abuses of that personal data.

V. (Personal) Data Access

Before any implementation, privacy issues should be considered in order to clearly identify who can access the personal data recorded in the EDRs and under which conditions (e.g. judicial warrant), particularly with regard to data subjects other than the driver, to whom (in principle) full and free access to his/her own data should be recognised. Appropriate and clear procedures should be established in order to allow data subjects to properly exercise their rights. A privacy and data protection impact assessment is considered a useful tool for this analysis.

VI. Data security and integrity

Standardized data security measures to prevent unlawful access, alteration or loss of EDR data need to be defined and universally adopted. Robust cryptographic techniques and proper authentication systems should be used to limit the risk of unintended data transfers or harmful attacks. The end-user should be able to verify, in a straight-forward manner, that EDRs and similar devices implemented in the vehicle are in full compliance with these standards. In a context of interconnected devices, stringent security measures are even more essential.

VII. Employee monitoring

In addition, laws relating to employee monitoring should be taken into account and fully respected when the employer installs devices which permit the monitoring of the driver's behaviour as well as the detection of the position of the vehicle (e.g. Journey Data Recorder or localisation systems).

50. Sitzung, 12. und 13. September 2011, Berlin

Arbeitspapier

Datenschutz und elektronisches Micropayment im Internet

Hintergrund

Öffentliche Äußerungen prominenter Medienunternehmen deuten darauf hin, dass sich die Ära der kostenfreien Nutzung von Online-Medien ihrem Ende nähern könnte. Verschiedene Anbieter von Online-Diensten und insbesondere Online-Zeitungen weltweit beginnen den Zugriff auf ihre Dienste ausschließlich gegen eine Gebühr anzubieten.

Die diskutierten Geschäftsmodelle reichen von Abonnements, bei denen ein Zugriff auf Basis einer monatlichen Gebühr angeboten wird, bis zu „pay per view"-Geschäftsmodellen, bei denen ein kleiner Geldbetrag für den Zugriff auf eine Einzelinformation gezahlt wird (sog. „Micropayment, z. B. für einen einzelnen Artikel in einer Online-Zeitung oder einen Video-Clip).

Zusätzlich gestattet die letze Generation von Mobiltelefonen die Installation von Zugriffsmöglichkeiten auf Online-Mediendienste über sog. „Apps". Verschiedene Anbieter von mobilen Endgeräten haben begonnen, eigene Verteilungsplattformen für solche „Apps" anzubieten, einschließlich damit verbundener Zahlungsdienste.

Gleichzeitig werden in sozialen Netzwerkdiensten sog. „Drittanwendungen" („Third-Party Applications") zunehmend populär. Viele dieser Drittanwendungen werden gegen Gebühr von einem anderen Anbieter als dem des sozialen Netzwerks angeboten. Facebook hat z. B. kürzlich die Einführung einer eigenen Währung „facebook coins" zum Bezahlen für Dienste innerhalb seines sozialen Netzwerks angekündigt.

Diese Entwicklungen können zu Beeinträchtigungen der Privatsphäre von Nutzern solcher Dienste führen, wenn die grundlegenden Prinzipien des Schutzes der Privatsphäre nicht beachtet werden. Tatsächlich haben die Anbieter solcher Micropayment-Systeme die Möglichkeit, Werbeeinnahmen durch die Auswertung der detaillierten personenbezogenen Transaktionsdaten zu generieren, die sie erlangen könnten.

Die Arbeitsgruppe hat bereits früher regelmäßig die Notwendigkeit der Wahrung der Anonymität im größtmöglichen Ausmaß als einen essentiellen Aspekt des

Schutzes der Privatsphäre im Internet betont[1]. Im Besonderen hat die Arbeitsgruppe die Notwendigkeit des Erhalts der Möglichkeit zum anonymen Zugriff auf digitale Medien, und besonders beim digitalen Fernsehen unterstrichen[2]. In jüngerer Zeit sind diese Prinzipien erneut in dem Konzept des „privacy by design" bestätigt worden[3],

Diese Prinzipien könnten gefährdet sein, wenn der Zugang zu Online-Medien und anderen Diensten gegen Gebühr angeboten wird, ohne dass anonyme Zahlungsmethoden zur Verfügung stehen. Wir könnten in eine Situation geraten, in der Nutzende sich allein zum Zweck der Bezahlung für einen Dienst identifizieren müssen.

Insbesondere besteht ein Risiko, dass „Micropayment"-Vorgänge (z. B. das Bezahlen für das Ansehen eines spezifischen Artikels in einer Online-Zeitung) zum Entstehen von Nutzungsdaten führen, die Spuren darüber enthalten, wer welchen Artikel in welchem Online-Medium zu welcher Zeit gelesen hat.

Gegenwärtig sind im Online-Bereich nur wenige Zahlungsmittel verfügbar, die denselben Grad von Anonymität wie Bargeld in der Offline-Welt haben. Die meisten der gängigen Zahlungsmethoden (z. B. Kreditkarten, Mobiltelefone, Zahlungsdiensteanbieter oder über Bankkonten) erlauben im Gegenteil keine anonyme Nutzung.

Während anonyme Guthabenkarten erhältlich sind, wird die Zahlung mit diesen Mitteln gegenwärtig nur von einer Minderheit von Online-Diensteanbietern angeboten.

Gleichzeitig ist in Deutschland ein Gesetzentwurf durch die deutsche Bundesregierung vorgelegt worden, der Anbieter von Online-Zahlungsdiensten zwingen würde, personalisierte Zahlungsmittel auch für Micropayment-Vorgänge anzubieten. Dies wird auf die Annahme gestützt, dass solche Dienste für Geldwäsche missbraucht werden könnten.

Empfehlungen

Im Lichte des oben Gesagten gibt die Arbeitsgruppe die folgenden Empfehlungen:

---

[1] Vgl. Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet – „Budapest-Berlin Memorandum", angenommen auf der 20. Sitzung in Berlin, Deutschland am 18./19. November 1996; http://www.datenschutz-berlin.de/attachments/137/bbmen_de.pdf

[2] Vgl. Arbeitspapier Datenschutz bei der Verbreitung digitaler Medieninhalte und beim digitalen Fernsehen, 42. Sitzung, Berlin, Deutschland, 4./5. September 2007; http://www.datenschutz-berlin.de/attachments/350/digit_de.pdf

[3] Vgl. 32. Internationale Konferenz der Datenschutzbeauftragten, Jerusalem, Israel, 27./29. Oktober 2010: Resolution zu privacy by design; http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

Gesetzgeber sollten von einem gesetzlichen Verbot von anonymen Mitteln zum Micropayment Abstand nehmen. Es muss möglich bleiben, alltägliche Einkäufe auch im Online-Bereich zu tätigen, ohne sich einzig für das Bezahlen identifizieren zu müssen.

Gesetzgeber sollten das Angebot anonymer oder wenigstens pseudonymer Bezahldienste – insbesondere für Micropayment-Vorgänge – in ihrer nationalen Gesetzgebung vorschreiben, wo dies nicht bereits der Fall ist. Dieser Gesichtspunkt sollte auch in dem laufenden Prozess der Evaluierung und möglichen Änderung nationaler und internationaler Instrumente zum Datenschutz in Betracht gezogen werden (z. B. der EU-Richtlinie 95/46, der Konvention 108 des Europarats oder der OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten).

Diensteanbieter sollten anonyme oder wenigstens pseudonyme Möglichkeiten zum Bezahlen ihrer Dienste anbieten. Sie sollten die Prinzipien des „privacy by design“ in ihren Angeboten von Anfang an berücksichtigen.

Nutzer von Online-Diensten, insbesondere von Online-Mediendiensten, sollten darauf hingewiesen werden, dass ihre Wahl einer Zahlungsmethode einen direkten Einfluss auf den Grad des Schutzes der Privatsphäre haben kann, der bei der Nutzung dieser Dienste garantiert werden kann. Sie sollten sich ausführlich über verschiedene verfügbare Zahlungsmethoden bei Diensteanbietern einzelner Plattformen informieren und anonyme oder wenigstens pseudonyme Bezahlungsmethoden fordern und wählen, wo immer dies möglich ist.

50th meeting, 12th and 13th September 2011, Berlin

Working Paper on Privacy and Electronic Micropayment on the Internet

Background

Public policy statements by prominent media organisations have signalled that the era of free online media may be nearing its end. Accordingly, several providers of online services, and specifically online newspapers, around the globe are beginning to offer access to their services exclusively on a fee paying basis.

The business models discussed range from subscription services where access would be offered for a monthly fee to "pay per view" business models where a small amount of money is paid for access to a single information item (so-called "micropayment", e. g. for an online newspaper article or video clip).

In addition, the latest generation of mobile devices provide the opportunity to install access capability to online media service via so-called "Apps". Several providers of mobile devices have started to offer their own distribution platforms for such "Apps", including related payment services.

At the same time, so-called "Third-Party Applications" are becoming increasingly popular in social network services. Many of these "Third-Party Applications" are being offered for a fee by a different service provider from the provider of the social network. Facebook, for example, has recently announced the introduction of its own currency "facebook coins" for paying for services inside its social network.

These developments can lead to infringements of the privacy of users of such services, if the basic principles for the protection of privacy are not being taken into account. Indeed, the providers of such micropayment systems have the opportunity to generate advertising revenue by exploiting the detailed personal transactional information that they may capture.

Previously, the Working Group has frequently stressed the need for the preservation of anonymity to the largest extent possible as an essential aspect of privacy protection on the Internet[1]. More specifically, the Working Group has underlined the need to maintain the possibility of anonymous access to digital media, and in particular digital television[2]. More recently, these principles have been reconfirmed in the concept of "privacy by design"[3].

These principles may be at risk when access to online media and other services is provided for a fee without anonymous payment methods being available. We may arrive at a situation where users will have to identify themselves solely for the purpose of being able to pay for a service.

---

[1] c.f. Report and Guidance on Data Protection and Privacy on the Internet – Budapest–Berlin Memorandum – adopted at 20th meeting in Berlin, Germany on 18/19 November 1996 (http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf)

[2] c.f. "Working Paper on Privacy Issues in the Distribution of Digital Media Content and Digital Television" – adopted at the 42nd meeting, Berlin, Germany on 4/5 September 2007; (http://www.datenschutz-berlin.de/attachments/349/digit_en.pdf?1201702193)

[3] Cf. 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-29 October, 2010: Resolution on Privacy by Design; http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

Specifically, there is a risk that "micropayment" operations (e.g. paying for viewing a specific article in an online newspaper) may generate traffic data that would include traces of who has read which article in which online media at which time.

At present, only a few payment means are available in the online environment which would allow for the same level of anonymity as cash in the offline world. On the contrary, most of the common payment methods (e. g. by credit cards, mobile phones, payment service providers, or via bank accounts) do not allow for anonymous use.

While anonymous prepaid cards are available, payment via these means is at present only offered by a minority of online service providers.

In addition, in Germany, a bill has been tabled by the German Federal Government that would force providers of online payment services to offer personalised payment means also for micropayment operations. This is based on the assumption that such services could be misused for money laundering.

Recommendations

In light of the above, the Working Group makes the following recommendations:

Regulators should refrain from prohibiting anonymous means for micropayments by law. It must remain possible to make everyday purchases without having to identify oneself solely for paying also in the online environment.

Regulators should mandate the provision of anonymous or at least pseudonymous payment services – specifically for micropayment operations – in their national legislation, where this is not already the case. This issue should also be taken into account in the ongoing process of evaluation and possible redrafting of national and international privacy instruments (e. g. the EU Directive 95/46, the Council of Europe Convention 108, or the OECD guideline on the protection of privacy and transborder flows of personal data).

Service providers should offer anonymous or at least pseudonymous means for payment for their services. They should take into account the principles of „privacy by design" in their services from the very outset.

Users of online services, especially of online media services, should be made aware that their choice of a payment method can have a direct impact on the level of privacy that can be guaranteed for the use of these services. They should carefully inform themselves about different payment methods available with service providers on certain platforms, and demand and choose anonymous or at least pseudonymous payment means wherever possible.

Arbeitspapier

Privacy by Design und Smart Metering: Minimierung personenbezogener Informationen zur Wahrung der Privatsphäre

Hintergrund

Aufgrund der kontinuierlichen Entwicklung des Smart Grids ändert sich die Rolle des Energieversorgungsbetriebs. Historisch gesehen stand bei den Energieversorgern die Aufrechterhaltung einer regelmäßigen Versorgung zu möglichst niedrigen Kosten im Vordergrund. Interaktionen mit Kunden bezogen sich weitgehend auf die Abrechnung und die Minimierung des Kreditrisikos. Doch mit der aktuellen Neugestaltung der elektrischen Systeme durchlaufen diese Interaktionen eine radikale Umgestaltung, da die Smart Meter es den Energieversorgern ermöglichen, so detailliert wie noch nie zuvor und fast in Echtzeit Informationen über das Nutzungsverhalten ihrer Privatkunden zu erlangen. Diese Änderung ermöglicht die Entwicklung einer Reihe neuer Dienstleistungen und Nutzwerte sowohl für die Verbrauchenden als auch die Energieversorger.

Zur Aufrechterhaltung des Vertrauens der Verbrauchenden werden das Smart-Grid und das Smart Metering die Entstehung einer neuen, auf Kundeneinbindung ausgerichteten Beziehung zwischen Versorgungsunternehmen und Privatpersonen erforderlich machen. Datenschutz und Datensicherheit werden die dualen Eckpfeiler dieser Beziehung sein.

Smart Meters

Im Rahmen des Smart Grids wird das Smart Meter die Technologie sein, die dem Verbrauchenden am meisten auffällt – der intelligente Zähler, der „wichtige erste Schritt“ auf dem Weg zu einem umfassenderen intelligenten Stromnetz als Ganzes.[1] Diese Messgeräte mit integrierter wechselseitiger Kommunikation und verbesserter individueller Nutzungsinformation werden den Energieverbrauchenden die Kontrolle und die Regulierung ihres eigenen Verbrauchs erlauben und es den Energieversorgern ermöglichen, eine bedarfsgerechte Versorgung zu gewährleisten und den Lastausgleich zu steuern. Sie werden ebenfalls eine wichtige Rolle bei der Entwicklung verbesserter Strategien zur Energieeinsparung spielen, um

[1] European Commission Staff Working Paper, Interpretative note on directive 2009/72/ec concerning common rules for the internal market in electricity and directive 2009/73/ec concerning common rules for the internal market in natural gas, p. 7, online: http://ec.europa.eu/energy/gas_electricity/interpretative_notes/doc/implementation_notes/2010_01_21_retail_markets.pdf

den internationalen Kampf gegen die Erderwärmung zu unterstützen, während sie den Verbrauchenden ermöglichen, ihren Verbrauch mit Hilfe von Informations- und Rückkoppelungssystemen zu reduzieren.[2] Ein Pike Forschungsbericht aus dem Jahr 2009 weist darauf hin, dass 250 Millionen intelligente Stromzähler weltweit bis zum Jahr 2015 installiert werden könnten.[3] Diese Zähler werden eine entscheidende Rolle in den fortgeschrittenen Mess-Infrastrukturen der Versorgungsunternehmen spielen, welche, ohne hier näher darauf einzugehen, ebenfalls die Integration angemessener Datenschutzmaßnahmen in den Systemen erfordern.

Es existiert keine standardisierte universelle Definition des Begriffs „Smart Meter"; vielmehr wurde der Begriff auf eine Vielzahl von Geräten angewandt, die unterschiedliche Funktionalitäten umfassen. Es gibt jedoch einige grundlegende gemeinsame Charakteristika bei den meisten aktuell entwickelten intelligenten Zählern. Als wesentlichste dieser Eigenschaften erweist sich die relativ feingranulare digitale Messung des Energieverbrauchs von Haushalten - zum Beispiel die Ablesung des Energieverbrauchs im Minutentakt. Aber auch eine gröbere Taktung wie die stündliche Ablesung ermöglicht die Erhebung von Intervallverbrauchsdaten, wodurch Zeittarif-Abrechnungen ermöglicht werden, die tageszeitabhängige Strompreisunterschiede beim Verbrauch berücksichtigen. Eine Digitalanzeige zum Energieverbrauch der Haushalte (z. B. aktueller Verbrauch pro Intervall oder zurückliegender Verbrauch pro Intervall) wird in der Regel mit der Möglichkeit zur Übermittlung dieser Informationen an ein anderes Gerät (z. B. Smartphone oder Fernsehen) vorhanden sein. Intelligente Messgeräte können auch mit einem internen Speicher ausgestattet sein, der die Speicherung aller Ablesungen aus einem Zeitraum von mindestens sechs Monaten ermöglicht.

Intelligente Messgeräte sind daneben tendenziell mit einer bidirektionalen Kommunikationsfunktionalität ausgestattet. Diese ermöglicht es den Versorgungsunternehmen, die Messgeräte aus der Ferne abzulesen (bei einer deutlichen Kostenreduzierung im Vergleich zu Messgeräten, die vor Ort durch einen Beschäftigten des Energieversorgers abgelesen werden). Diese Funktion ermöglicht den Verbrauchenden zunehmend die Kontrolle ihres Energieverbrauchs pro zurückliegendem Intervall in Online-Web-Portalen. Die bidirektionale Kommunikation erlaubt den Versorgungsunternehmen auch die Aktivierung von Lastausgleichsfunktionen, bei denen die Energieversorger den Energieverbrauch durch Kommunikation mit den intelligenten Messgeräten in teilnehmenden Haushalten ermitteln können. In einigen Rechtsräumen kann der Verbrauchende eine spezielle Einrichtung an

[2] Pacific Northwest National Laboratory: The Smart Grid: An Estimation of the Energy and CO2 Benefits. http://energyenvironment.pnnl.gov/news/pdf/PNNL-19112_Revision_1_Final.pdf

[3] Pike Research (Nov. 2, 2009) „Smart Meter Installations to Reach 250 Million Worldwide by 2015", online: http://www.pikeresearch.com/newsroom/smart-meter-installations-to-reach-250-million-worldwide-by-2015

das Gerät anschließen, die automatisch seinen / ihren Energieverbrauch basierend auf der Netzbelastung kontrolliert. Manche intelligenten Stromzähler mit bidirektionalen Kommunikationsfähigkeiten können auch mit einer ferngesteuerten Aktivierungs- und Deaktivierungsfunktion für die Versorgung ausgestattet sein. Dadurch kann ein Energieversorger mittels Fernsteuerung eine verbrauchende Person zu- oder abschalten.

Obwohl sich das Smart Metering bis heute auf den Verbrauch elektrischer Energie konzentriert, geht man davon aus, dass in der Zukunft die intelligenten Zähler auch für Wasser, Gas und Wärme eingesetzt werden. Dementsprechend sind einige intelligente Zähler darauf ausgelegt, die Messung für unterschiedliche Versorgungsunternehmen durchzuführen, um eine unnötige Verdoppelung der Infrastrukturen zu vermeiden.

Datenschutzrechtliche Probleme beim Smart Metering

Seit seiner Einführung haben sich Gesetzgeber, zahlreiche Datenschutzgruppen und Regulierungsbehörden auf die Notwendigkeit des Schutzes der Privatsphäre der Verbrauchenden beim Smart Grid konzentriert.[4] Es ist davon auszugehen, dass das Smart Grid bis zu acht Mal mehr Daten als das jetzige Stromnetz[5] generieren wird, die in einigen Fällen detaillierte Informationen über eine Person erkennen lassen könnten. Diese Intensivierung der Stromverbrauchsdaten ist verbunden mit dem Fernablesen und -erfassen der Daten, was Fragen in Bezug auf die Transparenz und die Kontrolle der Daten durch den Verbrauchenden aufwirft.[6]

Forschungsergebnisse deuten darauf hin, dass bei der Fortentwicklung des Smart Grids der Lebenswandel der Konsumierenden aus den generierten Informationen abgelesen werden kann –vor allem, da diese Informationen immer detaillierter werden und der charakteristische Stromverbrauch einzelner Geräten diese erkennbar macht. Doch selbst wenn der Stromverbrauch nicht im Minutentakt oder am Gerät aufgezeichnet wird, könnte die permanente Beobachtung des Stromverbrauchs die ungefähre Anzahl der Bewohner in einem Haushalt verraten, wann sie anwesend sind, sowie wann sie wach sind oder schlafen. Dies gefährdet die

[4] Beispiele sind die deutsche Energie-Gesetzgebung (Energiewirtschaftsgesetz – EnWG, zuletzt geändert am 28. Juli 2011, Bundesgesetzblatt I, S. 1690), the Information and Privacy Commissioner of Ontario, Canada's series of Smart Grid white papers, and The Article 29 Data Protection Working Party's „Opinion 12/2011 on Smart Metering (WP 183)." http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_de.pdf

[5] „Accenture Launches Smart Grid Data Management Solution to Reduce Risks and Costs of Smart Grid Deployments," Mar. 18, 2010, online: http://newsroom.accenture.com/article_display.cfm?article_id=4971

[6] Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs" http://www.datenschutz-berlin.de/attachments/717/80_DSK_Energieverbrauch.pdf?1288947505

Unverletzlichkeit der Wohnung, und solche intimen Details des täglichen Lebens erfordern ein hohes Schutzniveau. Diese Informationen sollten ohne das Wissen und das Einverständnis der/des Bewohner(s) nicht zugänglich sein. Die Verbrauchenden müssen die Möglichkeit und die Fähigkeit haben einzugreifen und zu bestimmen, wer auf diese Daten zugreifen darf. Prinzipiell sind alle offengelegten personenbezogenen Daten auf ein Mindestmaß zu beschränken, sowohl im Hinblick auf die Art und die Menge der Daten, als auch in Bezug auf die Übermittlung, die nur an die notwendigen Akteure erfolgen darf.

Die Bedeutung der Erhaltung des Vertrauens der Verbrauchenden in Bezug auf Datenschutz und Smart Metering wurde in vielen Rechtssystemen deutlich. Beispiele hierfür sind:

- **Kalifornien, USA:** Der Versorger PG & E wurde mit Blockaden von Anwohnern konfrontiert, die den Einbau intelligenter Zähler in ihrem Viertel verhindern wollten und sich dabei auf den Schutz der Privatsphäre und auf gesundheitliche Bedenken beriefen.[7]

- **British Columbia, Kanada:** Zahlreiche Beschwerden haben den Datenschutzbeauftragten der Provinz dazu veranlasst, eine Untersuchung von BC Hydro's Smart Meter-Programm ins Leben zu rufen. Dabei stellte er fest: „Datenschutz und Datensicherheit in Bezug auf die Energieverbrauchsdaten ist ein sehr reales Problem für die Bürger."[8]

- **Niederlande:** Ein Gesetzesentwurf aus dem Jahr 2006 wurde abgelehnt, der die obligatorische Einführung von Smart Metern vorsah. Dies geschah teilweise aufgrund eines Berichts, in dem festgestellt wurde, dass die Datenschutzbelange im Zusammenhang mit dem Gesetzesentwurf gegen Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) – Recht auf Achtung des Privat- und Familienlebens – verstoßen könnten.[9]

In diesen und anderen Fällen hätten vorausgehende Initiativen zur Entwicklung und zur Vermittlung des Datenschutzes sowie Schutzmaßnahmen für Smart-Meter-Systeme eine Schlüsselrolle dabei gespielt, Rückschläge in der Entwicklung zu vermeiden.[10]

[7] http://blogs.sfweekly.com/thesnitch/2010/12/smart_meters_west_marin.php

[8] http://www.oipc.bc.ca/news/2011Releases/NR_SmartMeters_28July2011.pdf

[9] http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf.

[10] http://download.pwc.com/ie/pubs/smart_from_start.pdf

Privacy by Design

In der gleichen Zeit, in der sich das Verhältnis zwischen dem Verbrauchenden und dem Energieversorger verändert hat und die Erhebung von Stromverbrauchsdaten erweitert worden ist, sind weltweit die Grundsätze des Privacy by Design (PbD) angenommen worden. Von seinen Ursprüngen Mitte der 90er Jahre entwickelte sich PbD zu einem weltweiten Standard, der durch eine einstimmig angenommene Entschließung der Internationalen Datenschutzkonferenz im Oktober 2010 als „ein wesentlicher Bestandteil des grundlegenden Schutzes der Privatsphäre" anerkannt worden ist. Der PbD-Standard, von Beginn an bei der Ausgestaltung Schutzvorrichtungen einzuplanen, wurde auch ein Gütesiegel bei Datenschutz- und Datensicherheitsbewertungen von Smart Grid und Smart Metering, siehe Anhang A.

Privacy by Design bietet Organisationen die Möglichkeit, unter Berücksichtigung der Privatsphäre von Anfang an ein positives Gesamtbild zu erzeugen und dabei Datenschutz- und Funktionalitätsanforderungen in Einklang zu bringen. Die Bewegung in Richtung des Smart Grid und insbesondere Smart Metering bildet in seinem aktuellen Entwicklungszustand eine ideale Plattform für die Anwendung von Privacy by Design. Nachstehend geben wir einige Empfehlungen für Smart Meter-Initiativen auf der Grundlage der *Best Practices for Privacy on the Smart Grid*.[11]

Empfehlungen

1. Smart Meter-Initiativen sollten in dem gesamten Rahmen der Projektführung Grundsätze des Datenschutzes aufweisen und proaktiv datenschutzrechtliche Anforderungen in ihre Entwicklung einbinden, um datenschutzgefährdenden Ereignissen vorzubeugen.

Energieversorger sollten Datenschutzverträglichkeitsprüfungen, sog. *Privacy Impact Assessments (PIAs)*, oder gleichartige Bewertungsverfahren als Teil der Anforderungen und der Entwicklungsstufen von Smart Meter-Initiativen durchführen. Innerhalb dieser Evaluierung sollten zwei wichtige Erwägungen angestellt werden. Zuerst sollten Versorgungsunternehmen festlegen, welche auf Smart Meter basierten Informationen für die rechtmäßigen Ziele *erforderlich* sind (und auf welcher Ebene der Identifizierbarkeit), und nicht, welche Informationen durch Smart Meter *verfügbar* sind. Sodann sollten Mechanismen eingesetzt werden, die den Verbrauchenden die Kontrolle über alle verfügbaren, nicht notwendigen Informationen ermöglichen. Zweitens sollten nur die zur Erfüllung der festgelegten Zwecke erforderlichen personenbezogenen Daten die Wohnung des Verbrauchen-

[11] http://www.privacybydesign.ca/content/uploads/2010/03/achieve-goldstnd.pdf

den über den intelligenten Stromzähler verlassen. Um sicherzustellen, dass die Verbrauchenden stets die Kontrolle über ihre Daten behalten, ist es wesentlich, dass sie vollständig über die Daten, die ihre Wohnungen verlassen, informiert werden. Sie sollten in die Lage versetzt werden, darüber zu bestimmen, welche Daten übermittelt werden, und gegebenenfalls eingreifen können.

Studien haben gezeigt, dass Versorgungsunternehmen keine detaillierten Informationen über den Stromverbrauch einzelner Verbrauchender benötigen, um den Netzlastausgleich zu schaffen. Um den Fluss personenbezogener Daten so gering wie möglich zu halten, können Energieversorger Verfahren wie Anonymisierung, Pseudonymisierung oder Datenaggregation anwenden.[12] Es sollten lokale Gateways (Schnittstellen) für einzelne Gebäude oder kleine Wohnviertel eingesetzt werden, die den Verbrauchenden einen Einblick in ihren Energieverbrauch gewähren, ohne dass die Übermittlung von Informationen über identifizierbare Verbrauchende an den Energieversorger nötig ist. Solche Gateways sollten in der Regel nicht von außen zugänglich sein und mit festgelegten Zugangskontrollprofilen arbeiten, während die Kommunikation auf dem push-Verfahren basierten sollte (die durch das Gateway initiiert wird). Andere Maßnahmen, wie zum Beispiel größere Intervalle zwischen den einzelnen Ablesungen, können ebenso verhindern, dass detaillierte Profile über die Lebensführung erstellt werden. Selbstverständlich werden hohe technische Standards für die sichere Speicherung und den Zugriff auf die Daten unerlässlich sein.

2. Smart Meter sollten zum Schutz der Privatsphäre idealerweise datenschutzfreundliche Grundeinstellungen enthalten, ohne dass es einer Handlung seitens des Verbrauchenden bedarf

Um den Datenschutz zu gewährleisten, sollte die Privatsphäre idealerweise durch datenschutzfreundliche Grundeinstellungen geschützt werden. Der Datenschutz sollte sich in dem Modus „keine Aktion erforderlich" befinden; der Verbrauchende sollte nur dann handeln müssen, wenn er über die Grundversorgungsleistungen hinausgehende Dienste nutzen möchte, für die die *Bekanntgabe* weiterer Daten erforderlich ist, nicht aber für den *Schutz* der personenbezogenen Daten. Hier sollten zumindest zwei besondere Überlegungen angestellt werden. Erstens sollte, wenn dem Verbraucher mehrere Optionen angeboten werden (entweder im Hinblick auf die Art des Zählers oder auf dessen Grundeinstellung), die Standardeinstellung die datenschutzfreundlichste Einstellung sein. Zweitens sollte, selbst wenn sich die Verbrauchenden für eine detaillierte Erfassung ihrer Verbrauchsdaten durch die intelligenten Zähler entschieden haben, vor jeder einzelnen Nutzung

[12] Vgl. z. B. Kursawe, K., Danezis, G, Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid; and Jawurek, M., Johns, M., and Kerschbaum, F. (2011) Plug-in privacy for Smart Metering billing; beide in Fischer-Hübner, S. and Hopper, N (Eds): *Proceedings of the 11th Privacy Enhancing Technologies Symposium*, Waterloo, ON, July 2011

oder Weitergabe dieser Daten für andere als die Primärzwecke die informierte, positive Einwilligung dieser Personen eingeholt werden.

3. Der Datenschutz sollte ein wesentlicher Bestandteil bei der Ausgestaltung von Smart Meter-Systemen und -Anwendungen sein

Da Smart Meter-Initiativen in immer mehr Rechtssystemen weltweit zu finden sind, werden eine Reihe von Best Practices der Wirtschaft und rechtliche Anforderungen entwickelt. Diese werden die Bemühungen der Energieversorger und Dritter vorantreiben, datenschutzfreundliche Verfahren für die Erhebung, Nutzung und Übermittlung von Informationen aus den intelligenten Stromzählern zu schaffen. Die Regulierungsbehörden sollten als Grundsätze festlegen, dass die Verbrauchenden volle Transparenz und die Möglichkeit erhalten, den Fluss personenbezogener Daten zu kontrollieren und zu bestimmen. Detaillierte Muster über den Energieverbrauch des Einzelnen sollten nur der betroffenen Person zugänglich sein, es sei denn, diese gibt die Daten weiter.

Allerdings darf der Datenschutz nicht nur auf den rechtlichen oder administrativen Schutz angewiesen sein; er sollte ebenfalls in die Gestaltung der Technologie einfließen. An dem Scheidepunkt der Datenerhebung können Smart Meter eine maßgebliche Rolle dabei spielen zu definieren, welche Daten in das größere Smart Grid-Ökosystem gelangen, und in welcher Form dies geschieht.

4. Smart Meter-Initiativen sollten unnötige Kompromisse zwischen dem Datenschutz und anderen zulässigen Funktionen oder organisatorischen Zielen vermeiden

Datenschutz sollte nicht als Widerspruch zu der Funktionsvielfalt der intelligenten Stromzähler betrachtet werden. Die Verbrauchenden sollten nicht gezwungen werden, sich zwischen Datenschutz und Energieeffizienz/-einsparung zu entscheiden; vielmehr müssen Versorgungsunternehmen durch den Einsatz von *Privacy by Design* sicherstellen, dass alle gesetzmäßigen Ziele (einschließlich des Datenschutzes) in den Smart Meter-Initiativen erreicht werden.

5. Datenschutz und Datensicherheit sollten durchgehend aufrechterhalten werden – Schutz während des gesamten Lebenszyklus

Daten aus intelligenten Stromzählern – insbesondere solche, die einer Person zugeordnet werden können – sollten gut geschützt werden, sowohl bei der Speicherung als auch bei der Übermittlung. Dies erfordert die Entwicklung und Durchführung von Datensicherungsmaßnahmen auf dem Smart Meter selbst (wobei

bestmöglich gewährleistet sein muss, dass das Gerät manipulationssicher ist und nicht mehr Daten als notwendig speichert), während der Datenübermittlung (Verschlüsselung, Anonymisierung, Identifikation und Schutz der Metadaten), und während der Verarbeitung und Nutzung (auf das erforderliche Maß beschränkter Zugriff auf Daten, Sicherstellung, dass Dritte entsprechende Schutzstandards erfüllen, sichere Löschung am Ende der Nutzungsdauer etc.).

6. Smart Meter-Initiativen sollten erkennbar und transparent sein und rechenschaftspflichtige Geschäftspraktiken anwenden; gegenüber den Verbrauchenden sollte nachgewiesen werden, dass die Technologie in Übereinstimmung mit den festgelegten Zielen betrieben wird

Energieversorger sollten nachweisen können, dass die angewandten Methoden zur Integration des Datenschutzes in ihren Smart Meter-Initiativen den datenschutzrechtlichen Anforderungen des Projekts gerecht werden. Indem die Nachweisbarkeit der Einhaltung der Vorgaben grundlegender Datenschutzprinzipien in jeder Phase einer Smart Meter-Initiative sichergestellt ist, wird gewährleistet, dass der Energieversorger jederzeit für einen Audit durch Dritte bereit ist.

Für die Verwirklichung von Sichtbarkeit und Transparenz sind wichtige Grundsätze, dass die Verbrauchenden über die Verwendung der von intelligenten Zählern erhobenen personenbezogenen Daten informiert werden und ein durchsichtiger und zugänglicher Beschwerdeprozess eingerichtet wird. Die Verbrauchenden sollten die einfache technische Möglichkeit zur Festlegung von Zugangskontrollprofilen erhalten, um so zu bestimmen, wer welche personenbezogenen Daten erhält.

7. Smart Meter-Initiativen sollten so gestaltet sein, dass sie den Verbrauchendendatenschutz berücksichtigen – die Nutzenden sollen im Mittelpunkt stehen

Die Verbrauchenden sollten alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten und entsprechende Erklärungen erhalten, um ihren Energieverbrauch und ihren Datenschutz regeln zu können.

8. Rechtliche Rahmenbedingungen sollten die Einführung und die Nutzung des datenschutzfreundlichen Einsatzes von Smart Meter fördern.

Die in den vorstehenden Empfehlungen dargestellten Grundsätze sollten in national und international verbindliche Regelungen aufgenommen werden, sofern dies noch nicht geschehen ist.

ANHANG A –
Beispiele von *Privacy by Design* in Smart Grid-Konsultationsdokumenten

- **Expert Group 2:** „Wenn der Datenschutz während der Ausgestaltungsphase des Smart Grid (‚Privacy by Design') berücksichtigt wird, ist es möglich, daraus nutzer- und unternehmensfreundliche Lösungen zu entwickeln"; „Seien Sie sich über das zukünftige Einschleichen von Funktionen bewusst und integrieren Sie Datenschutz- und Datensicherheitsaspekte frühzeitig in die Entwicklung durch die Anwendung der ‚Privacy (and Security) by Design'-Prinzipien"[13]

- **Artikel 29-Arbeitsgruppe:** „Die Einführung intelligenter Verbrauchsmessverfahren muss so erfolgen, dass der Datenschutz von Anfang an mit einbezogen wird, und zwar nicht nur hinsichtlich der Sicherheitsmaßnahmen, sondern auch dadurch, dass die Menge der verarbeiteten personenbezogenen Daten minimiert wird."[14]

- **Europäische Kommission:** „Die Task Force ‚Intelligente Netze' ist übereingekommen, dass ein ‚Privacy-by-Design'-Ansatz erforderlich ist. Dieser Ansatz wird in die Normen eingearbeitet werden, die von den europäischen Normungsgremien entwickelt werden."[15]

- **Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Deutschland):** „Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen."[16]

- **Public Interest Energy Research (PIER) Programm:** „Datenschutzrechtliche Erwägungen müssen Entscheidungen zur Architektur und zur Ausgestaltung des Informationsflusses innerhalb dieses Netzwerks antreiben, genauso wie die Strategien zu Smart Grid-Daten, die von einer zunehmenden Anzahl von Einheiten gehalten werden, was sich bei der Erzielung des Nutzens dieser Investition als hilfreich erweisen wird. Da der Datenschutz in die technische Entwicklung integriert werden muss, kann er keine angemessene Berücksichtigung finden, wenn Richtlinien erst nach der vollständigen Entwicklung der Technologien geschaffen werden."[17]

[13] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

[14] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_de.pdf

[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:DE:PDF

[16] http://www.datenschutz-berlin.de/attachments/717/80_DSK_Energieverbrauch.pdf?1288947505

[17] http://hes-standards.org/doc/SC25_WG1_N1475.pdf

- **Trans-Atlantic Consumer Dialogue (TACD):** „Unterstützen Sie den Datenschutz und die Datensicherheit durch die Ausgestaltung, einschließlich der Datenminimierung, Anonymisierung und Aggregation sowie Modellen, bei denen die Kontrolle der Verbrauchenden über ihre Energieverbrauchsdaten im Vordergrund steht.“[18]

- **National Institute of Standards and Technology (NIST):** „Aufgrund des großen Vertrauens in die Technologie den Informationsaustausch muss die Berücksichtigung von Datenschutzrisiken ein Teil des heutigen Geschäftsmodells sein, und die Erwägung der Auswirkungen auf den Datenschutz sollte einen Teil der täglichen Geschäftsaktivitäten ausmachen.“[19]

- **Ontario (Canada) Minister of Energy Directive:** „Respektieren und schützen Sie die Privatsphäre der Kunden. Integrieren Sie frühzeitig Datenschutzanforderungen in die Planung und Gestaltung von Smart-Grids, einschließlich der Ausführung von Abschätzungen der Auswirkungen auf die Privatsphäre (Privacy Impact Assessments)“.[20]

- **Center for Democracy and Technology & Electronic Frontier Foundation:** „Die Annahme von Datenschutzbestimmungen, die den gesamten Satz an fairen Informationspraktiken umsetzen, wird jetzt, zu Beginn des Einsatzes von Smart Grids, für solide und anpassungsfähige Rahmenbedingungen für den Einbau des Datenschutzes in die sich weiter entwickelnden Smart Grids sorgen. Dadurch bekommen Versorgungsunternehmen und Innovatoren ein festes Rahmenwerk, auf dem sie aufbauen können.“[21]

- **Smart Grid Canada:** „Der erfolgreiche Einsatz von Smart Grid beruht letztlich auf dem Vertrauen der Verbrauchenden. Datenschutzrechtliche Bedenken und andere öffentliche Belange, die eine Bedrohung für das Vertrauen der Verbrauchenden darstellen, müssen angegangen werden. Es ist von höchster Priorität, die Probleme in Bezug auf die Integrität zu bestimmen, die Entwicklung von Lösungen und Standards auszuweiten und sie in die in Kanada eingesetzten Smart-Grid-Produkte und -Dienstleistungen einzubauen.“[22]

[18] http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=294&Itemid=

[19] http://epic.org/privacy/smartgrid/NIST_Smartgrid_Priv_Guidelines.pdf

[20] http://www.wise.uwaterloo.ca/SmartGrid/Minister_directive_smart_grid_20101123.pdf

[21] http://www.eff.org/files/PoliciesandProcedures_15Oct2010_OpeningComment.pdf

[22] http://sgcanada.org/media/2011/04/Smart-Grid-Priorities-for-Canada-in-2011.pdf

Working Paper

Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy

Background

With the ongoing growth of the Smart Grid, the role of the utility is changing. Historically, energy providers focused on maintaining consistent supply at the lowest possible cost; interactions with customers largely involved billing and minimizing credit risk. However, with the current redesign of electrical systems, these interactions are being radically redesigned, as smart meters allow utilities to gain information about the usage patterns of their residential customers at a level of detail that was previously unavailable, and in near real-time. This change is allowing for the development of an array of new services and efficiencies for both the consumer and the utility.

To maintain consumer trust and confidence, the Smart Grid and smart metering will necessitate the emergence of a new relationship between utilities and individuals, centred on customer engagement. Privacy and data security will be the dual cornerstones of this relationship.

Smart Meters

When looking at the Smart Grid, the technology that will be most apparent to consumers will be the smart meter – the "essential first step" toward the implementation of a broader Smart Grid as a whole.[1] These meters, which incorporate two-way communications and enhanced individual usage information, will allow energy consumers to control and regulate their own consumption and utilities to enable demand response and load balancing functions. They will also play a key role in the development of improved power savings strategies to support the international fight against global warming, while allowing consumers to reduce consumption through information and feedback systems[2]. A 2009 Pike Research

[1] European Commission Staff Working Paper, Interpretative note on directive 2009/72/EC concerning common rules for the internal market in electricity and directive 2009/73/EC concerning common rules for the internal market in natural gas, p. 7, online: http://ec.europa.eu/energy/gas_electricity/interpretative_notes/doc/implementation_notes/2010_01_21_retail_markets.pdf

[2] Pacific Northwest National Laboratory: The Smart Grid: An Estimation of the Energy and CO2 Benefits. http://energyenvironment.pnnl.gov/news/pdf/PNNL-19112_Revision_1_Final.pdf

report suggests that 250 million smart meters could be installed worldwide by 2015.[3] These meters will play an integral role in utilities' overall Advanced Metering Infrastructures, which, while not further discussed here, will also require the incorporation of appropriate privacy protections at the system level.

There is no standard, universal definition for the term 'smart meter'; in fact, the term has been applied to a variety of devices that incorporate different functionalities. There are, though, certain basic characteristics shared by most smart meters currently deployed. The most fundamental of these qualities is the digital metering of household energy consumption at a relatively fine level of granularity – minute-by-minute readings of energy used, for instance. Even a less fine level of granularity, such as hourly readings, allows for the collection of 'interval consumption' data which enables the possibility of Time-of-Use billing, by which different energy rates are applied based on the time at which energy was consumed. A digital readout displaying household energy consumption data (such as current or historic interval consumption) will generally be present, along with a means of communicating this information to another device (e.g. a smartphone or television). Smart meters may also be equipped with internal memory sufficient to enable the storage of all readings for at least a 6 month period.

Smart meters also tend to be equipped with bi-directional communication functionality. This allows utilities to remotely read the meters (at a significantly reduced cost as compared to meters being read onsite by a utility employee), and increasingly is enabling consumers to monitor their historic interval consumption via online web portals. Bi-directional communication also allows utilities to enable 'load balancing' functions, in which the utility can mediate energy consumption through communications with smart meters in participating households. In some jurisdictions, the consumer can install a special device on an appliance that automatically controls its energy consumption based on the network load. Some smart meters with bi-directional communication capabilities may also be equipped with remote enablement and disablement of supply functionality, enabling a utility to remotely connect or disconnect a consumer.

Although smart metering to date has been focused on electrical power consumption, it is anticipated that smart meters may also be used for water, gas and heat. Accordingly, some smart meters are being designed to support metering of multiple utilities in order to avoid unnecessary duplication of infrastructure.

[3] Pike Research (Nov. 2, 2009) "Smart Meter Installations to Reach 250 Million Worldwide by 2015", online: http://www.pikeresearch.com/newsroom/smart-meter-installations-to-reach-250-million-worldwide-by-2015

Smart Meter Privacy Issues

Since its introduction, legislators, numerous privacy groups and regulatory agencies have focused on the need to protect consumer privacy in the Smart Grid[4]. The Smart Grid is expected to generate up to eight orders of magnitude more data than the current power network[5] which, in some cases, could reveal detailed information about a person. This increase in electrical consumption data is paired with remote reading and collection of the data, raising issues with regard to transparency and consumer control of data.[6]

Research suggests that as the Smart Grid matures, consumer lifestyles could be gleaned from the information generated – particularly as this information becomes more granular, and the power consumption signatures of appliances become recognizable. However, even if electricity use is not recorded minute by minute, or at the appliance level, ongoing monitoring of electricity consumption may reveal the approximate number of occupants in a household, when they are present, as well as when they are awake or asleep. This may jeopardize the sanctity of the home, and such intimate details of daily life require a high level of protection. This information should not be accessible without the knowledge and consent of the occupant(s). The consumer must have the opportunity and ability to intervene and to determine who can access this data. In principle, any personal data disclosed must be minimized, in terms of both type and quantity of data disclosed and disclosure only to necessary parties.

The importance of maintaining consumer trust and confidence with respect to privacy and smart metering has been seen in numerous jurisdictions. Examples include:

- **California, USA**: Utility PG&E has faced blockades by residents looking to prevent the installation of smart meters in their neighbourhoods, citing privacy and health concerns.[7]

- **British Columbia, Canada**: Numerous complaints have prompted the province's Information and Privacy Commissioner to launch an investigation of

[4] Examples include the German energy legislation (Energiewirtschaftsgesetz – EnWG, last amended on 28 July 2011, Bundesgesetzblatt I, S. 1690), the Information and Privacy Commissioner of Ontario, Canada's series of Smart Grid white papers, and The Article 29 Data Protection Working Party's "Opinion 12/2011 on Smart Metering (WP 183)." http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

[5] "Accenture Launches Smart Grid Data Management Solution to Reduce Risks and Costs of Smart Grid Deployments," Mar. 18, 2010, online: http://newsroom.accenture.com/article_display.cfm?article_id=4971

[6] Resolution of the 80th Conference of the Data Protection Commissioners of the Federation and of the Länder (Nov. 3-4, 2010), "Data protection in connection with digital metering and control of energy consumption." http://www.datenschutz-berlin.de/attachments/823/Appendix_2.pdf

[7] http://blogs.sfweekly.com/thesnitch/2010/12/smart_meters_west_marin.php

BC Hydro's smart meter program, noting "the privacy and security of energy consumption data is a very real issue for citizens."[8]

- **Netherlands:** A 2006 bill proposing the mandatory rollout of smart meters was rejected, in part due to a report that found that the privacy concerns associated with the bill might have violated the Article 8, respect for one's private and family life, of the European Convention on Human Rights.[9]

In these cases and others, upfront initiatives to develop and communicate data privacy and protection measures for smart metering systems would have played a key role in avoiding deployment setbacks. [10]

Privacy by Design

Concurrent to the change in the consumer-utility relationship and the collection of increasing power usage information is the global adoption of the principles of *Privacy by Design (PbD)*. From its origins in the mid-90s, *PbD* has become a worldwide standard, being recognized as "an essential component of fundamental privacy protection" through an International Resolution unanimously passed at the International Data Protection and Privacy Commissioners' Conference in October 2010. The *PbD* standard of designing protections in from the outset has also become a hallmark of privacy and security analyses of the Smart Grid and Smart Metering, as shown in Appendix A.

Privacy by Design is providing organizations with a means to, by considering privacy from the outset, achieve a positive-sum scenario – meeting both privacy and functionality requirements. The movement towards the Smart Grid and, in particular, smart metering, in its current nascent state, is at an ideal stage for the application of *Privacy by Design*. Below, we offer a number of recommendations for smart metering initiatives, based on the *Best Practices for Privacy on the Smart Grid*[11].

Recommendations

1. **Smart metering initiatives should feature privacy principles in the overall project governance framework and proactively embed privacy requirements into their design, in order to prevent privacy-invasive events from arising.**

[8] http://www.oipc.bc.ca/news/2011Releases/NR_SmartMeters_28July2011.pdf

[9] http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf.

[10] http://download.pwc.com/ie/pubs/smart_from_start.pdf

[11] http://www.privacybydesign.ca/content/uploads/2010/03/achieve-goldstnd.pdf

Utilities should conduct Privacy Impact Assessments (PIAs) or similar type assessments as part of the requirements and design stages of smart metering initiatives. Within this evaluation, two important considerations should be made. First, utilities should make a determination of what smart meter-based information is *required* to meet legitimate objectives (and at what level of identifiability), rather than of what information is made *available* by smart metering. Mechanisms should then be put in place to allow consumers to maintain control over any available, non-necessary information. Secondly, only the personal information necessary for the determined purposes should leave the consumer's home via the smart meter. In order to ensure that consumers always retains control over their data it is essential that they are fully informed about the data which leave their homes. They should have the possibility to determine which data is sent and to intervene if necessary.

Some research has shown that utilities may not need detailed energy consumption information about individual consumers to perform load balancing functions. To achieve as little personal data flow as possible utilities may use techniques such as anonymisation, pseudonymisation, or data aggregation[12]. Local gateways for individual buildings or small neighbourhoods, which allow the consumer to gain insight into their energy usage without the need for transmission of information about identifiable consumers to the utility, should be applied. Such gateways should generally not be externally-accessible and work with defined access protection profiles, while communication should be push-based (initiated by the gateway). Other measures, such as larger intervals between individual readings, can also prevent a detailed profile about the consumer's life-style from being generated. Of course, high technical standards for securely storing and accessing the data will be essential.

2. Smart meters should ideally protect privacy by default, with no action required on the part of the consumer

In order to ensure its presence, privacy should ideally be protected as the default condition. Privacy should be in a 'no action required' mode; consumer action should only be required for the *disclosure* of data exceeding core utility services, not the *protection* of personal information. At least two particular considerations should be made here. First, where multiple options (with regard to either the type of meter or its initial settings) are presented to the consumer, the default option should be the more privacy-protective one. Secondly, even where consumers have opted to have detailed consumption information collected by the smart meter, the

[12] For instance, see Kursawe, K., Danezis, G, and Johlweiss, M. (2011) Privacy-Friendly Aggregation for the Smart-Grid; and Jawurek, M., Johns, M., and Kerschbaum, F. (2011) Plug-in privacy for Smart Metering billing; both in Fischer-Hübner, S. and Hopper, N (Eds): *Proceedings of the 11th Privacy Enhancing Technologies Symposium*, Waterloo, ON, July 2011

informed, positive consent of those individuals should be sought prior to each separate use or disclosure of this information for non-primary purposes.

3. Privacy should be an essential design feature of smart meter systems and practices

As smart metering initiatives are seen in an increasing number of jurisdictions worldwide, a number of industry best practices and legislative requirements are under development. These will enhance the efforts of utilities and third-parties to create privacy-friendly practices for the collection, use and disclosure of smart meter-based information. Regulators should state the main principles that the consumer should have full transparency and the ability to control and determine the flow of personal data. Detailed patterns of an individual's energy consumption should only be accessible to the data subject, unless he or she shares them further.

However, privacy cannot be solely reliant on legislative or administrative protections; it should also be designed into the technology itself. As the point of collection, smart meters can play a clear role in defining what data will enter the larger Smart Grid ecosystem, and the form in which it will do so.

4. Smart metering initiatives should avoid unnecessary trade-offs between privacy and other legitimate functionalities or organizational objectives

Privacy should not be considered to be 'at odds' with the functionality of smart meters. Consumers should not be forced into a choice between privacy and energy efficiency/conservation; utilities should ensure, through the use of *Privacy by Design*, that all legitimate objectives (including privacy) are met in smart metering initiatives.

5. Privacy and data security should be maintained end-to-end – full lifecycle protection

Smart meter-based information – particularly personally identifiable information – should be strongly protected, whether at rest or in transit. This requires the development and implementation of data protections at the smart meter itself (ensuring, to the extent possible, that the device is tamperproof, and that it does not store more data than necessary), during transmission of the data (encryption, anonymisation, identification and protection of metadata), and during processing and use (minimized access to data, ensuring third parties meet equivalent protection standards, secure destruction at end-of-life, etc.).

6. Smart metering initiatives should be visible and transparent, and should utilize accountable business practices; consumers should be assured that the technology operates in accordance with stated objectives

Utilities should be able to show that the methods used to incorporate privacy into their smart metering initiatives will meet the privacy requirements of the project. Ensuring such 'requirements traceability' between the foundational privacy principles and each stage of a smart metering initiative will ensure that the utility is ready for a third part audit at any time.

Informing consumers of the use to which personal information collected from smart meters will be put, and the establishment of a clear and accessible complaints process, are key objectives in achieving visibility and transparency. Consumers should be given the simple technical option to define access control profiles and thus determine who receives what personal information.

7. Smart metering initiatives should be designed to respect consumer privacy – keep it user-centric.

Consumers should be provided with, and educated about, all necessary information, options and controls to allow them to manage their energy consumption and their privacy.

8. Regulatory frameworks should foster the introduction and use of privacy-friendly smart meter and smart grid applications.

The concepts laid out in the recommendations above should be incorporated into national and international regulatory frameworks where this is not already the case.

APPENDIX A –
Examples of *Privacy by Design* in Smart Grid consultation documents

- **Expert Group 2:** "If privacy is addressed at the design phase of the Smart Grid ('privacy by design'), it is possible to derive user and business friendly solutions"; "Be aware of future function creep and incorporate privacy and security considerations early on in the development by applying 'privacy (and security) by design' principles"[13]

- **Article 29 Working Group:** "Smart metering implementation should take place with privacy built in at the start, not just in terms of security measures, but also in terms of minimising the amount of personal data processed"[14]

- **European Commission:** "The Smart Grids Task Force has agreed that a 'privacy by design' approach is needed. This will be integrated in the standards being developed by the ESOs [European Standards Organizations]."[15]

- **Data Protection Commissioners of the Federation and of the Länder (Germany):** "Data protection must be guaranteed already when planning and designing the infrastructure for energy metering and the technical equipments."[16]

- **Public Interest Energy Research (PIER) Program:** "Privacy considerations must drive architectural and information flow design decisions within the network, as well as the policies that cover Smart Grid data held by the growing array of entities that will help reap the benefit of this investment. Because privacy must be embedded in technical design, it cannot be addressed adequately by policies created once technologies have matured."[17]

- **Trans-Atlantic Consumer Dialogue (TACD):** "Encourage privacy and security by design, including data minimization, anonymisation, and aggregation, and models that focus on consumers' maintaining control of their utility consumption data."[18]

---

[13] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

[14] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF

[16] Resolution of the 80th Conference of the Data Protection Commissioners of the Federation and of the Länder (Nov. 3-4, 2010), "Data protection in connection with digital metering and control of energy consumption." http://www.datenschutz-berlin.de/attachments/823/Appendix_2.pdf

[17] http://hes-standards.org/doc/SC25_WG1_N1475.pdf

[18] http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=294&Itemid=

- **National Institute of Standards and Technology (NIST):** "With heavy reliance upon technology and information sharing, addressing privacy risks must be part of the business model today, and consideration of privacy impacts should be part of everyday business activities."[19]

- **Ontario (Canada) Minister of Energy Directive:** "Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments."[20]

- **Center for Democracy and Technology & Electronic Frontier Foundation:** "Adopting privacy rules implementing the full set of [Fair Information Practices] now, at the beginning of Smart Grid deployment, will provide a sound and adaptable framework for designing privacy into the Smart Grid as it develops, giving utilities and innovators a solid framework upon which to build."[21]

- **Smart Grid Canada:** "The successful deployment of smart grid ultimately relies on consumer confidence and trust, privacy and other public concerns that threaten to undermine consumer confidence need to be addressed. It is an immediate priority to define the integrity issues, escalate the development of solutions and standards, and embed them into smart grid products and services deployed in Canada.[22]

[19] http://epic.org/privacy/smartgrid/NIST_Smartgrid_Priv_Guidelines.pdf

[20] http://www.wise.uwaterloo.ca/SmartGrid/Minister_directive_smart_grid_20101123.pdf

[21] http://www.eff.org/files/PoliciesandProcedures_15Oct2010_OpeningComment.pdf

[22] http://sgcanada.org/media/2011/04/Smart-Grid-Priorities-for-Canada-in-2011.pdf

2012

51. Sitzung, 23. und 24. April, Sopot, Polen

Arbeitspapier zu Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes

– *„Sopot Memorandum “* –

Anwendungsbereich

In diesem Arbeitspapier wird insbesondere die Verarbeitung personenbezogener Daten beim Cloud Computing untersucht.

Nicht betrachtet werden Szenarien, in denen alle Endnutzer, der für die Verarbeitung Verantwortliche, der Auftragsdatenverarbeiter und alle Unterauftragnehmer denselben Datenschutzregeln unterliegen, physisch im selben Hoheitsgebiet angesiedelt sind und jegliche Datenverarbeitung und -speicherung in diesem Hoheitsgebiet erfolgt. Das Arbeitspapier ist ebenfalls weniger relevenat, wenn der Cloud-Dienst unter der vollständigen Kontrolle des Nutzers dieses Dienstes ist.

Schließlich befasst sich das Arbeitspapier nur mit der Nutzung von Cloud-Diensten durch Unternehmen und Behörden, die bestehende Verfahren „in die Cloud“ verlagern, und nicht mit der Nutzung dieser Dienste durch Privatpersonen.

Allgemeiner Hintergrund

„Cloud Computing ist ein sich entwickelndes Paradigma.“[1]

Cloud Computing (CC) stößt auf wachsendes Interesse, da es eine höhere Wirtschaftlichkeit, geringere Umweltbelastung, einen einfacheren Betrieb, höhere Benutzerfreundlichkeit und eine Reihe weiterer Vorteile verspricht.

Im September 2011 erschien die Sonderveröffentlichung SP 800-145 des National Institute of Standards and Technology (NIST), in der Cloud Computing wie folgt definiert wird:

[1] National Institute of Standards and Technology (NIST), Special Publication 800–145, *The NIST Definition of Cloud Computing*, September 2011, Seite 2.

„Cloud Computing ist ein Modell zur Ermöglichung eines ubiquitären, komfortablen, auf Abruf verfügbaren Netzzugriffs auf einen gemeinsamen Pool aus konfigurierbaren Rechenressourcen (z. B. Netze, Server, Speicher, Anwendungen und Dienste), der schnell und mit geringfügigem Verwaltungsaufwand bzw. minimaler Interaktion mit dem Dienstanbieter bereitgestellt und öffentlich verfügbar gemacht werden kann. Das Cloud-Modell besteht aus fünf wesentlichen Charakteristika, drei Service- und vier Nutzungsmodellen.“[2]

Unter anderem soll die Definition

„als Ausgangspunkt für eine Diskussion darüber dienen, was Cloud Computing ist und wie es am besten genutzt werden kann.“[3]

Die Definition trägt zu einem besseren Verständnis davon bei, was CC eigentlich ist. Dieses Verständnis entwickelt sich derzeit rasant. Die Definition des NIST ist ein hervorragender Ausgangspunkt für die weitere Untersuchung des CC und seiner Nutzung.

Allerdings gibt es auch immer noch Unklarheiten im Zusammenhang mit CC, insbesondere hinsichtlich des Datenschutzes und anderer rechtlicher Fragen. Die Empfehlungen in diesem Arbeitspapier sollen helfen, diese Unklarheiten zu verringern.

Im ersten Teil werden zunächst die Empfehlungen vorgestellt. Der zweite Teil enthält weitere Hintergrundinformationen über Cloud Computing und Begründungen für die Empfehlungen. Wer sich näher mit dem Thema auseinandersetzen möchte, sollte diesen Teil zuerst lesen.

Für die Zwecke dieses Arbeitspapiers ist der für die Verarbeitung Verantwortliche der Kunde und der Auftragsverarbeiter der Cloud-Anbieter.[4]

Die Entwicklung des CC har eine Reihe wichtiger Themen hervorgehoben, z. B.:

a. Es gibt noch keine internationale Einigung auf eine einheitliche Terminologie;

b. Die Technologie befindet sich noch in der Entwicklung;

c. Riesige Datenmengen werden zusammengetragen und gebündelt;

---

[2] National Institute of Standards and Technology (NIST), Special Publication 800–145, *The NIST Definition of Cloud Computing*, September 2011, Seite 3.

[3] National Institute of Standards and Technology (NIST), Special Publication 800–145, *The NIST Definition of Cloud Computing*, September 2011, Seite 2.

[4] Vgl. Nr. 39 und 40 unten. Die Unterauftragnehmer des Cloud-Anbieters gelten im Zusammenhang mit der Verarbeitung personenbezogener Daten ebenfalls als Auftragsverarbeiter.

d. Die Technologie ist grenzenlos und grenzüberschreitend[5];

e. Daten werden weltweit verarbeitet;

f. Die Prozesse, Verfahren und Methoden der Cloud-Anbieter sind nicht ausreichend transparent, z. B. ob Cloud-Anbieter Unteraufträge für die Verarbeitung vergeben und wenn ja, welche Prozesse, Verfahren und Methoden diese verwenden;

g. Dieser Mangel an Transparenz erschwert eine angemessene Risikobewertung.

h. Aufgrund dieses Mangels an Transparenzist es auch schwerer, Datenschutzregeln durchzusetzen.

i. Die Cloud-Anbieter stehen unter einem großen Druck, möglichst schnell Kapital aus den hohen Investitionskosten zu schlagen.

j. Die Kunden stehen unter einem zunehmenden, teilweise der weltweiten Finanzkrise geschuldeten Druck, die Kosten auch für ihre Datenverarbeitung zu senken.

k. Um die Preise niedrig zu halten, sind Cloud-Anbieter eher bereit, allgemeine Geschäftsbedingungen anzubieten.

Daraus können sich folgende **Risiken** ergeben:

A. Verletzungen der Informationssicherheit, wie die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von (personenbezogenen) Daten werden vom Verantwortlichen für die Verarbeitung nicht erkannt.

B. Daten werden in Hoheitsgebiete übertragen, die keinen angemessenen Datenschutz gewährleisten.

C. Verstöße gegen Gesetze und Grundsätze des Schutzes der Privatsphäre und des Datenschutzes.

D. Der für die Verarbeitung Verantwortliche akzeptiert allgemeine Geschäftsbedingungen, die dem Cloud-Anbieter zu viel Spielraum lassen, u. a. die Möglichkeit, Daten entgegen den Anweisungen des für die Verarbeitung Verantwortlichen zu verarbeiten.

[5] Vgl. Nr. 38

E. Verwendung von Daten des für die Verarbeitung Verantwortlichen für eigene Zwecke ohne Wissen oder Erlaubnis des für die Verarbeitung Verantwortlichen durch Cloud-Anbieter oder ihre Unterauftragnehmer.

F. Die Rechenschaftspflicht und Verantwortung wird in einer Kette von Unterauftragnehmern scheinbar ausgehöhlt oder verschwindet.

G. Der für die Verarbeitung Verantwortliche verliert die Kontrolle über die Daten und die Datenverarbeitung.

H. Der für die Verarbeitung Verantwortliche oder ein vertrauenswürdiger Dritter (z. B. Prüfer) ist nicht in der Lage, den Cloud-Anbieter angemessen zu kontrollieren.

I. Datenschutzbehörden werden davon abgehalten, die Verarbeitung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen und den Cloud-Anbieter angemessen zu überwachen.

J. Der für die Verarbeitung Verantwortliche verlässt sich aufgrund mangelnder Informationen und Überwachung auf ungerechtfertigtes Vertrauen und verstößt dadurch möglicherweise gegen geltendes Datenschutzrecht im Niederlassungsland.

Die **folgenden Empfehlungen** sollen zur **Verringerung der Risiken bei der Nutzung von Cloud-Diensten beitragen und verantwortungsvolles Handeln fördern**[6], so dass die Vorteile der Verwendung von CC genutzt werden können, jedoch nicht auf Kosten der Rechte des Einzelnen.

Empfehlungen[7]

Allgemeine Empfehlungen

Die Arbeitsgruppe empfiehlt, dass:

- durch Cloud Computing Datenschutzstandards im Vergleich zur herkömmlichen Datenverarbeitung nicht abgesenkt werden **dürfen**;

[6] Auf den Seiten 9 und 10 ihres Berichts *Cloud Computing – Benefits, risks and recommendations for information security* [Cloud Computing: Nutzen, Risiken und Empfehlungen zur Informationssicherheit] vom November 2009 nennt die ENISA die häufigsten Sicherheitsrisiken. Dazu zählen in zufälliger Reihenfolge: Kontrollverlust, Abhängigkeit von einem Anbieter (Lock-in-Effekt), fehlende Isolation, Datenschutz, unsichere oder unvollständige Löschung von Daten, interne Angreifer. Weitere Einzelheiten können dem Bericht entnommen werden. Hier wird der Kontrollverlust betont.

[7] Die Liste der Empfehlungen ist nicht abschließend.

- die für die Verarbeitung Verantwortlichen vor dem Einstieg in CC-Projekte eine Abschätzung der Folgen für den Datenschutz und eine Risikoabschätzung vornehmen (ggf. mithilfe vertrauenswürdiger Dritter).

- Anbieter von Cloud-Diensten ihre Verfahren weiterentwickeln, um mehr Transparenz, Sicherheit, Nachprüfbarkeit und Vertrauen in CC-Lösungen zu schaffen, insbesondere im Hinblick auf Informationen über mögliche Verstöße gegen den Datenschutz und ausgewogenere Vertragsbedingungen zur Förderung der Portabilität von Daten und der Kontrolle über die Datendurch die Cloud-Nutzer.

- Weitere Bemühungen in der Forschung, der Zertifizierung durch Dritte, der Standardisierung, von „Privacy by Design"-Technologien und anderen damit verbundenen Bereichen unternommen werden, um das gewünschte Vertrauen in CC zu erreichen.

- Gesetzgeber überprüfen, ob das bestehende Recht zur grenzüberschreitenden Datenübertragung weiterhin angemessen ist, und zusätzliche Datenschutzvorkehrungen im Bereich des CC in Erwägung ziehen[8].

- Datenschutzbehörden die für die Verarbeitung Verantwortlichen, Cloud-Anbieter und Gesetzgeber weiterhin über Fragen des Schutzes der Privatsphäre und des Datenschutzes informieren.

Weitere Hinweise zu bewährten Verfahren („best practices")

1. CC sollte in sorgfältigen, maßvollen Schritten umgesetzt werden, beginnend mit nicht-sensiblen und nicht-vertraulichen Daten.

2. Die Verarbeitung sensitiver[9] Daten über CC stößt auf zusätzliche Bedenken. Unbeschadet nationaler Gesetze erfordert diese Art der Verarbeitung zusätzliche Schutzmaßnahmen.

3. Für die Verarbeitung Verantwortliche und Datenschutzbehörden sollten Zugang zu **standortbezogenen Audit Trails** haben. Der Audit Trail sollte automatisch aufgezeichnet werden und anzeigen, an welchen physischen

[8] Vgl. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre: Entschließung über Internationale Standards zum Schutz der Privatsphäre („Entschließung von Madrid"), 5. November 2009; http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

[9] Der Begriff der sensitiven Daten ist in verschiedenen Rechtskulturen unterschiedlich besetzt: vgl. Art. 8 der Richtlinie 95/46/EG, Art. 9 des Entwurfs der Datenschutzverordnung sowie den FTC-Bericht „Protecting Comsumer Privacy in an Era of Rapid Change" (2012).

Standorten personenbezogene Daten zu welchen Zeitpunkten gespeichert oder verarbeitet wurden[10].

4. Ein **automatisch aufgezeichneter Audit Trail über Kopier- und Löschvorgänge sollte** eingerichtet werden, anhand dessen eindeutig erkennbar ist, welche Kopien personenbezogener Daten der Auftragsverarbeiter oder seine Unterauftragnehmer angelegt und gelöscht haben.

5. Die Audit Trails zur Protokollierung des Standorts sowie der Kopier- und Löschvorgänge sollten auch die Datensicherung umfassen.

6. Wirksame technische Maßnahmen sollten entwickelt werden, um eine rechtswidrige Übertragung personenbezogener Daten in Hoheitsgebiete ohne ausreichenden Datenschutz zu verhindern.

7. Es sollte sichergestellt werden, dass personenbezogene Daten wirksam von Laufwerken und anderen Speichermedien **gelöscht** werden, z. B. durch **sofortiges Überschreiben mit Zufallsdaten**[11].

8. Es sollte sichergestellt sein, dass ruhende Daten und die Datenübertragung[12] mithilfe anerkannter Standardalgorithmen und aktueller Schlüssellängen **verschlüsselt** werden. Die Schlüssel sollten von keinem anderen als dem für die Verarbeitung Verantwortlichen und den Cloud-Anbieter verwendet werden und nur diesen zugänglich sein. Die Schlüssel sollten nicht von anderen Kunden als denen des Cloud-Anbieters verwendet werden oder diesen zugänglich sein. Daten sollten nicht länger und in größerem Umfang in unverschlüsselter Form zugänglich sein als für die jeweilige Datenverarbeitung unbedingt nötig. Methoden, mit deren Hilfe Daten für CC-Anbieter zu jeder Zeit **unlesbar** gemacht werden können, sollten weiter untersucht werden[13]. Es könnte nützlich sein, Möglichkeiten zu erkunden, wie der für die Verarbeitung Verantwortliche die Entschlüsselung von Daten durch den Cloud-Anbieter und seine Unterauftragnehmer wirksam und schnell unterbinden kann (Notbremse).

[10] Der standortbezogene Audit Trail könnte beispielsweise eine klare Übersicht darüber geben, wann die einzelnen personenbezogenen Daten an bestimmten Standorten ein- und ausgetragen wurden und wann sie zu welchen Standort übertragen werden.

[11] Eine Löschung durch Dereferenzierung der Daten und späteres Überschreiben durch Wiederverwendung der Speicherbereiche reicht in der Regel nicht aus, da weiterhin die Möglichkeit besteht, dass Daten vor oder während der Wiederverwendung der Speicherbereiche durch erneute Referenzierung wieder zugänglich werden.

[12] Während der Datenübertragung sollte eine Ende-zu-Ende-Verschlüsselung erfolgen. Es muss sichergestellt sein, dass personenbezogene Daten während der Übertragung gegen aktive (z. B. Replays, Traffic Injection) und passive Angriffe (z. B. Belauschen) geschützt sind. Ferner muss der Datenzugriff durch unbefugte Dritte mithilfe entsprechender technischer und organisatorischer Verfahren verhindert werden (z. B. Zugangskontrolle, Datenverschlüsselung).

[13] Ein Forschungsbeispiel in diesem Bereich ist die Sealed Cloud, welche im Preprint des Artikels von Hubert A. Jäger und Arnold Monitzer „Sealed Cloud – a novel approach to defend insider attacks“ beschrieben ist. Der Preprint kann unter der folgenden Adresse aufgerufen werden http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf.

9. Alle Verwendungen personenbezogener Daten durch Cloud-Anbieter und ihre Unterauftragnehmer sollten automatisch **protokolliert** werden. Das Protokoll sollte für den für die Verarbeitung Verantwortlichen leicht zugänglich sowie einfach und leicht verständlich gestaltet sein. Der Cloud-Anbieter und seine Unterauftragnehmer sollten die Integrität der Protokolle gewährleisten.

Verantwortliche für die Verarbeitung

10. Der für die Verarbeitung Verantwortliche sollte in die Vereinbarung mit dem Cloud-Anbieter eine vollständige Liste mit Informationen über alle physischen Standorte aufnehmen, an denen über die Laufzeit der Vereinbarung Daten durch den Cloud-Anbieter und/oder seine Unterauftragnehmer gespeichert oder verarbeitet werden, einschließlich zur Datensicherung (**Grundsatz der Standorttransparenz**).

11. Der für die Verarbeitung Verantwortliche sollte in der Vereinbarung sicherstellen, dass weder der Cloud-Anbieter noch seine Unterauftragnehmer, ungeachtet ihrer Gründe und ob die Daten verschlüsselt werden, Daten an andere Standorte als die im Vertrag aufgelisteten übertragen. Dies sollte von technischen Maßnahmen begleitet werden, deren Vorhandensein und Zuverlässigkeit der für die Verarbeitung Verantwortliche tatsächlich prüfen kann.

12. Der für die Verarbeitung Verantwortliche sollte dafür sorgen, dass die Vereinbarung mit dem Cloud-Anbieter unmissverständlich ist und keine Auslegungen zulässt, die den Grundsatz untergräbt, dass der Cloud-Anbieter personenbezogene Daten nur entsprechend den Weisungen des für die Verarbeitung Verantwortlichen verarbeitet. Können Cloud-Anbieter die Vereinbarung einseitig ändern, sollte der für die Verarbeitung Verantwortliche das Recht haben, den Vertrag zu kündigen und die Daten an einen anderen Cloud-Anbieter zu übertragen.

13. Die Vereinbarung sollte ausdrücklich regeln, dass der Cloud-Anbieter die Daten des für die Verarbeitung Verantwortlichen nicht für seine eigenen Zwecke nutzen darf.

14. Der für die Verarbeitung Verantwortliche sollte die Möglichkeit haben, alle Standorte, an denen personenbezogene Daten ganz oder teilweise verarbeitet werden, in der Vergangenheit verarbeitet wurden oder gemäß der Vereinbarung in Zukunft verarbeitet werden, zu prüfen oder prüfen zu lassen. Die Vereinbarung sollte festlegen, dass der für die Verarbeitung Verantwortliche das Recht hat, vollständige Informationen über alle Aspekte des Cloud-Anbieters und seiner Unterauftragnehmer zu erhalten, die der für die Verarbeitung Verantwortliche als notwendig erachtet, um die Einhaltung der Vereinbarung zu gewährleisten, d. h. zu gewährleisten, dass die Verarbeitung personenbezo-

gener Daten in Einklang mit den Weisungen und geltendem Recht sowie auf angemessen sichere Art und Weise erfolgt.

15. Der für die Verarbeitung Verantwortliche sollte sich in der Vereinbarung das Recht sichern, die Verarbeitung personenbezogener Daten durch den Cloud-Anbieter und ggf. seine Unterauftragnehmer durch einen vertrauenswürdigen Dritten (z. B. ein anerkanntes Prüfunternehmen)[14] vollständig oder teilweise überwachen zu lassen.

16. Vor dem Einsatz von CC sollte der für die Verarbeitung Verantwortliche auf der Grundlage seiner Informationen über die Bedingungen und Umstände, unter denen personenbezogene Daten vom Cloud-Anbieter und ggf. seinen Unterauftragnehmern verarbeitet werden, eine **Risikoabschätzung** vornehmen. Die Risikoabschätzung sollte alle Standorte umfassen, an denen personenbezogene Daten verarbeitet oder gespeichert werden. Setzt der Cloud-Anbieter für Teile der Verarbeitung Unterauftragnehmer ein, sollte die Risikoabschätzung auch alle Standorte der Unterauftragnehmer umfassen.

17. Der für die Verarbeitung Verantwortliche sollte die Risikoabschätzung regelmäßig überprüfen und aktualisieren, solange personenbezogene Daten vom Cloud-Anbieter verarbeitet werden.

18. Vor dem Einsatz von CC sollte der für die Verarbeitung Verantwortliche versuchen sicherzustellen, dass ein Ausstieg aus dem Cloud-Dienst tatsächlich möglich ist, wozu auch eine aktive Rolle des Cloud-Anbieters beim Transfer der Daten zählt, um nicht von einem Cloud-Anbieter abhängig zu werden (Lock-in-Effekt).

19. Der für die Verarbeitung Verantwortliche sollte prüfen, ob es notwendig ist, sich den Zugriff auf mindestens eine nutzbare Kopie der Daten außerhalb der Kontrolle, des Zugriffs oder des Einflusses des Cloud-Anbieters (und seiner Unterauftragnehmer) zu sichern. Falls ja, sollte die Kopie unabhängig von der Mitwirkung des Cloud-Anbieters und seiner Unterauftragnehmer für den Verantwortlichen für die Verarbeitung zugänglich und nutzbar sein.

20. Der für die Verarbeitung Verantwortliche sollte im Falle eines **Verletzung der Datensicherheit** seine Verpflichtungen gegenüber den Betroffenen und den Datenschutzbehörden vollständig erfüllen und geeignete Maßnahmen ergreifen können. Von daher sollte der für die Verarbeitung Verantwortliche klare Vereinbarungen mit dem Cloud-Anbieter über die umgehende und umfassende Benachrichtigung des für die Verarbeitung Verantwortlichen und/oder der Datenschutzbehörde im Falle einer solchen Verletzung treffen.

[14] Das Thema vertrauenswürdige Dritte ist in Nr. 44 näher beschrieben.

21. Der für die Verarbeitung Verantwortliche sollte den Cloud-Anbieter vertraglich dazu verpflichten, wirksame und schnelle Verfahren umzusetzen, damit die Betroffenen ihr Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten wahrnehmen können.

Cloud-Anbieter

22. Der Cloud-Anbieter sollte gegenüber dem für die Verarbeitung Verantwortlichen vollständige Transparenz bezüglich der von ihm und ggf. seinen Unterauftragnehmern verwendeten Standorte für die Verarbeitung und Speicherung personenbezogener Daten gewährleisten.

23. Der Cloud-Anbieter sollte vollständige Transparenz bezüglich seiner Unterauftragnehmer und der von ihnen durchgeführten Verarbeitungsprozesse gewährleisten.

24. Der Cloud-Anbieter sollte Transparenz in Vertragsfragen gewährleisten und CC nicht mit allgemeinen Geschäftsbedingungen anbieten, die einseitige Vertragsänderungen ermöglichen.

25. Cloud-Anbieter und ggf. ihre Unterauftragnehmer werden ermutigt, sich nach bewährten Verfahren zu richten und es einem unparteiischen Dritten zu erlauben, sie zu vergleichen und zu bewerten (Benchmarking).

26. Allgemeine Geschäftsbedingungen für bestimmte Marktsegmente, z. B. kleine und mittelständische Unternehmen, sollten so gestaltet sein, dass die Achtung der Privatsphäre und angemessene Schutzmaßnahmen berücksichtigt werden.

Prüfungen

27. Da ein Cloud-Anbieter sehr große Mengen an personenbezogenen Daten ansammeln kann, sollte der Cloud-Anbieter im Interesse des für die Verarbeitung Verantwortlichen zusätzlich zu dessen Prüfungen auch von einer dritten Stelle überprüft werden. Der Prüfer sollte vollkommen unabhängig vom Cloud-Anbieter sein und der Sicherheit der Verarbeitung personenbezogener Daten besondere Aufmerksamkeit schenken. Der Prüfer sollte insbesondere prüfen, ob Maßnahmen in den folgenden Bereichen ergriffen wurden und ordnungsgemäß funktionieren: standortbezogener Audit Trail (vgl. Nr. 3), Audit Trails für das Kopieren und Löschen (vgl. Nr. 4), Löschung (vgl. Nr. 7) und Protokollierung (vgl. Nr. 9). Ferner sollte der Prüfer prüfen, ob folgende Maßnahmen ergriffen wurden und ordnungsgemäß funktionieren: Maßnah-

men zur Verhütung der rechtswidrigen Datenübertragung in Hoheitsgebiete ohne ausreichenden Datenschutz (vgl. Nr. 6) und Maßnahmen zur Verhütung der Datenübertragung an andere Standorte als die ausdrücklich mit dem Kunden vereinbarten (vgl. Nr. 10 und 11). Schließlich sollte der Prüfer sicherstellen, dass es dem Cloud-Anbieter oder ggf. seinen Unterauftragnehmern nicht möglich ist, diese Maßnahmen unentdeckt zu umgehen.

Hintergrundinformationen zu den Empfehlungen

28. CC ist eine recht **neue Form** der Datenverarbeitung, die sich aus der mangels einer besseren Benennung **traditionelle Datenverarbeitung** genannten Form der Datenverarbeitung entwickelt hat. Es hat sich eine langjährige, solide Erfahrung mit der traditionellen Datenverarbeitung angesammelt, doch gibt es keine derartige solide Erfahrung mit CC.

29. Die Folge dieses **Paradigmenwechsels** ist, dass Grundannahmen, Erfahrungen, Ideen, Theorien und Modelle für die Datenverarbeitung nicht mehr mit der Praxis übereinstimmen und daher einer kritischen Prüfung, Neubewertung und ggf. Überarbeitung unterzogen werden müssen. Dies trifft auch auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten sowie die Art und Weise zu, wie **Risiken** analysiert, bewertet und beurteilt werden können. Die bewährten Verfahren von gestern sind nicht unbedingt die bewährten Verfahren von heute.

30. Die **neue Situation** muss untersucht und in **sorgfältig gewählten Schritten** umgesetzt werden, insbesondere hinsichtlich des Datenschutzes und des Schutzes der Rechte der Betroffenen im weiteren Sinne.

31. Die **technische Grundlage** des CC ist eine ausgereifte Netzwerktechnik und Server-Virtualisierung. Dies ermöglicht eine schnelle und dynamische Verlagerung von Daten und deren Verarbeitung lokal zwischen Servern im jeweiligen Rechenzentrum und global zwischen Servern in weltweiten Rechenzentren. Die Technologie ist hochgradig skalierbar, ohne einschränkende Engpässe zu erzeugen. Das Internet ermöglicht es dem Endnutzer, unabhängig vom Standort der Rechenzentren auf die Daten zuzugreifen.

32. Die **wirtschaftliche Antriebskraft** hinter CC sind **Skaleneffekte**. Die Zusammenfassung der Datenverarbeitung in großen Zentren verbessert die Nutzung teurer Ressourcen, wie z. B. menschlichem Wissen, Sachwerten (Hardware, Software, Gebäude), von Kommunikationsbandbreite und Energie. Aufgrund ihrer Größe und ihres Volumens haben Cloud-Anbieter zudem eine besonders starke Verhandlungsposition beim Erwerb von Ressourcen. Somit können Cloud-Anbieter Stückkosten reduzieren und den Kunden attraktive

Preise anbieten. Um Skaleneffekte erzielen zu können, müssen möglichst viele Kunden den Dienst nutzen. Um ein ausreichendes **Volumen** zu erreichen, werden Cloud-Dienste weltweit über das Internet angeboten.

33. CC gilt als große Chance für kleine und mittelständische Unternehmen, Zugang zu bezahlbaren und skalierbaren Rechenressourcen zu erhalten. Aufgrund der großen Anzahl relativ kleiner Organisationen wird erwartet, dass Cloud-Anbieter allgemeine Geschäftsbedingungen für dieses Marktsegment entwickeln.

34. CC ist viel dynamischer als die traditionelle Datenverarbeitung. Der Standort, an dem Daten verarbeitet werden, kann sich stark verändern. Der aktuelle Standort von Daten und ihrer Verarbeitung kann von verschiedenen Faktoren abhängen, über die sich Endnutzer und für die Verarbeitung Verantwortliche bisher wenig Gedanken gemacht haben und über die sie unter Umständen wenig wissen und wenig Kontrolle haben. Beispielsweise siedeln Cloud-Anbieter ihre Datenzentren häufig in verschiedenen Ländern und auf mehreren Kontinenten an, u. a. aufgrund einer günstigen Stromversorgung, eines kühlen Klimas und unterschiedlicher Zeitzonen. Unvorhersehbare Umstände, z. B. Ausfälle in einem Rechenzentrum oder ein Kapazitätsmangel bei Spitzenlasten (Überlauf), können auch Einfluss auf den aktuellen Standort von Daten haben. Kopien von Daten können an andere Datenzentren übertragen werden, um die Online-Verfügbarkeit im Falle von Störungen in einem Datenzentrum zu gewährleisten oder Sicherungskopien zu erstellen (Redundanz).

35. CC beruht auf vielen Kunden, die dynamisch einen gemeinsamen Pool an Ressourcen des Cloud-Anbieters nutzen. Dies sollte jedoch nur geschehen, wenn eine **klare Trennung** der verschiedenen Kundendaten und ihrer Verarbeitung aufrechterhalten werden kann. Die gemeinsame Nutzung von Ressourcen birgt ein höheres Risiko für umfangreiche Verluste oder die unbefugte Offenlegung von Daten.[15] Das Risiko erhöht sich auch dadurch, dass CC von der Kostenoptimierung durch ein großes Datenvolumen angetrieben wird (Skaleneffekt). Cloud-Kunden stellen ein Risiko für einander dar. Je mehr Kunden auf dieselben Ressourcen zugreifen, desto größer wird das Risiko für jeden einzelnen Kunden und somit für alle Cloud-Kunden zusammen.

36. Das Wissen über CC und Informationen über seine Risiken konzentrieren sich derzeit auf einige wenige große Cloud-Anbieter, die anscheinend aus

[15] Auf den Seiten 9 und 10 ihres Berichts *Cloud Computing – Benefits, risks and recommendations for information security* [Cloud Computing: Nutzen, Risiken und Empfehlungen zur Informationssicherheit] vom November 2009 nennt die ENISA die häufigsten Sicherheitsrisiken. Dazu zählen in zufälliger Reihenfolge: Kontrollverlust, Abhängigkeit von einem Anbieter (Lock-in-Effekt), fehlende Isolation, Datenschutz, unsichere oder unvollständige Löschung von Daten, interne Angreifer. Weitere Einzelheiten können dem Bericht entnommen werden. An dieser Stelle sei darauf hingewiesen, dass fehlende Isolation als eines der größten Risiken angesehen wird.

wirtschaftlichen oder wettbewerblichen Gründen nur zögerlich Informationen über bestimmte Bedingungen und Umstände an die Öffentlichkeit weitergeben. Die ungleiche Verteilung von Wissen und Informationen zwischen Cloud-Anbietern und Kunden versetzt letztere in eine schwächere Position beim Abschluss von Vereinbarungen und erschwert es ihnen, die Risiken der beabsichtigten Nutzung von CC angemessen zu bewerten.

37. Eine gründliche **Risikoabschätzung** muss auf **dem Verständnis des** konkreten Aufbaus und der konkreten Umstände des Cloud-Dienstes an allen Standorten beruhen, an denen Daten verarbeitet werden.

38. Die CC-Technologie ist **grenzenlos** und **grenzüberschreitend**. Der weltweite Kundenstamm, gepaart mit der weltweiten Verteilung von Rechenzentren und dem dynamischen Strom von Daten (und von Datenverarbeitung) kann dazu führen, dass Daten nationale Grenzen überschreiten und Hoheitsgebiete mit einem damit einhergehenden Mangel an Transparenz wechseln. Personenbezogene Daten können in Datenzentren in Hoheitsgebieten ohne angemessenen Datenschutz gelangen oder kommerziell missbraucht werden, oder ausländische Mächte greifen ohne Berechtigung darauf zu.[16]

39. Im Sinne des Datenschutzes muss zwischen den einander ausschließenden Rollen des für die Verarbeitung Verantwortlichen und des Auftragsdatenverarbeiters unterschieden werden. Der **für die Verarbeitung Verantwortliche** legt den Zweck und die Mittel für einen bestimmten Vorgang der Datenverarbeitung fest.

40. Allgemein anerkannt ist auch, dass ein für die Verarbeitung Verantwortlicher die Verarbeitung personenbezogener Daten durch einen **Auftragsdatenverarbeiter** erlauben kann, dies jedoch nur in Einklang mit den ausdrücklichen **Weisungen** des für die Verarbeitung Verantwortlichen.

41. Ein allgemein anerkannter Grundsatz des Datenschutzes ist, dass der Auftragsdatenverarbeiter personenbezogene Daten nicht in größerem Umfang verarbeiten darf, als sich aus den ausdrücklichen Weisungen des für die Verarbeitung Verantwortlichen ableiten lässt[17]. Für das CC bedeutet dies, dass ein Cloud-Anbieter keine einseitige Entscheidung treffen oder die mehr oder weniger automatische Übertragung personenbezogener Daten (und ihrer Verarbeitung) an unbekannte Rechenzentren veranlassen kann. Dies gilt

[16] Zwar können personenbezogene Daten in einem Hoheitsgebiet verarbeitet werden, doch kann der Cloud-Anbieter oder das Mutterunternehmen in einem anderen Hoheitsgebiet angesiedelt sein, was es ausländischen Strafverfolgungsbehörden ermöglichen würde, auf die Daten im Cloud-Dienst zuzugreifen, auch wenn die Daten physisch außerhalb der geografischen Grenzen dieses Landes gespeichert sind. Hierzu könnte der Abschluss eines internationalen Abkommens notwendig sein.

[17] Oder durch Gesetz.

unabhängig davon, ob der Cloud-Anbieter eine solche Übertragung mit der Verringerung der Betriebskosten, der Bewältigung von Spitzenlasten (Überlauf), der Lastenverteilung, der Erstellung von Sicherungskopien usw. begründet. Noch darf der Cloud-Anbieter personenbezogene Daten für seine eigenen Zwecke nutzen[18].

42. Ein weiterer allgemein anerkannter Grundsatz des Datenschutzes erfordert, dass der für die Verarbeitung Verantwortliche geeignete **technische und organisatorische Sicherheitsmaßnahmen** ergreift, um Daten vor versehentlicher oder rechtswidriger Zerstörung, Verlust oder Schädigung, sowie vor unbefugter Offenlegung, Missbrauch oder anderen Arten der Verarbeitung, die gegen gesetzliche Bestimmungen verstoßen, zu schützen. Dasselbe gilt für Auftragsdatenverarbeiter.

43. Um seiner Verantwortung gerecht zu werden, muss der für die Verarbeitung Verantwortliche die Verarbeitung durch den Auftragsdatenverarbeiter **überwachen**, um sicherzustellen, dass sie entsprechend seiner Anweisungen erfolgt und dabei angemessene Sicherheitsmaßstäbe eingehalten werden.

44. Ohne seine Verantwortung abzutreten kann der für die Verarbeitung Verantwortliche ausdrückliche Anweisungen geben, dass die Überwachung der Verarbeitung durch den Auftragsverarbeiter teilweise von einem **vertrauenswürdigen Dritten** (z. B. einem Prüfer) übernommen wird. Bedingung ist, dass der Dritte über die notwendigen Qualifikationen verfügt, unabhängig vom Auftragsverarbeiter ist, vollen Zugang zu und vollständigen Einblick in die Bedingungen und Umstände der Verarbeitung durch den Auftragsverarbeiter hat und dem für die Verarbeitung Verantwortlichen zuverlässig über seine Beobachtungen, Bewertungen und Schlussfolgerungen berichten kann.

Die Arbeitsgruppe wird die Entwicklungen im Bereich des Cloud Computing weiter verfolgen und das vorliegende Arbeitspapier ggf. aktualisieren.

[18] Verarbeiten Cloud-Anbieter Daten ohne Wissen des für die Verarbeitung Verantwortlichen, sollte der Cloud-Anbieter als Mitverantwortlicher für die Verarbeitung angesehen und als solcher für die unbefugte, unabhängige Datenverarbeitung zur Rechenschaft gezogen werden.

51st meeting, 23rd and 24th April 2012, Sopot, Poland

Working Paper on Cloud Computing – Privacy and data protection issues – *"Sopot Memorandum"* –

Scope

This working paper specifically examines the processing of personal data in cloud computing environments.

The working paper does not examine a situation in which all end users, the controller, the processor and all of its subcontractors are subject to the same data protection legislation and are physically located within the same jurisdiction and all data processing and data storage takes place within this jurisdiction. This paper is also of less relevance, where the cloud service is totally under the control of the cloud service user.

Finally, the working paper only deals with the use of cloud services by companies and public authorities which move existing procedures "into the cloud", not with the use of such services by individuals.

General Background

"Cloud computing is an evolving paradigm."[1]

Cloud Computing (CC) is attracting increasing interest due to promises of greater economic efficiency, lower environmental impact, simpler operation, increased user-friendliness and a number of other benefits.

In September 2011, the National Institute of Standards and Technology (NIST) released Special Publication SP 800–145, in which it defined cloud computing as:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly

[1] National Institute of Standards and Technology (NIST), Special Publication 800–145, *The NIST Definition of Cloud Computing*, September 2011, Page 2.

provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." [2]

The definition is, among other things,

"…… intended …… to provide a baseline for discussion from what is cloud computing to how to best use cloud computing."[3]

The definition is an important contribution to the ongoing process of understanding what CC actually is. This understanding is developing rapidly. The NIST definition is an excellent starting point for further investigation of CC and how to use it.

However, there is still uncertainty in relation to CC, especially when it concerns privacy, data protection and other legal issues. The recommendations in this paper are intended to help reduce that uncertainty.

The paper is structured to present the recommendations first. The second part of the paper provides additional background on cloud computing as well as the rationale behind the recommendations. For deeper insight, readers might benefit from reading this section first.

For the purposes of this paper, the cloud customer is deemed to be the data controller and the cloud service provider is deemed to be the data processor.[4]

The evolution of CC has highlighted a number of important issues, including:

a. there is not yet international agreement on common terminology;

b. the development of the technology is still in progress;

c. enormous amounts of data are being accumulated and concentrated;

d. the technology is boundless and transboundary[5];

e. data processing has become global;

[2] National Institute of Standards and Technology (NIST), Special Publication 800–145, *The NIST Definition of Cloud Computing*, September 2011, Page 3.

[3] National Institute of Standards and Technology (NIST), Special Publication 800–145, *The NIST Definition of Cloud Computing*, September 2011, Page 2.

[4] Cf. paras. 39 and 40 below. The cloud service provider's subcontractors in connection with the processing of personal data are also considered processors.

[5] Cf. para. 38.

f. transparency is lacking with respect to cloud service provider processes, procedures and practices, including whether or not cloud service providers subcontract any of the processing and if so, what their respective processes, procedures and practices are;

g. this lack of transparency makes it difficult to conduct a proper risk assessment;

h. this lack of transparency also makes it more difficult to enforce rules regarding data protection;

i. cloud service providers are under great pressure to quickly capitalise significant investment costs;

j. cloud customers are under increasing pressure to reduce costs, including those of their data processing, in part accelerated due to the global financial crisis; and

k. to keep low prices cloud service providers are more likely to offer standard terms and conditions.

These circumstances may lead to **an increased risk of**:

A. breaches of information security such as breaches of confidentiality, integrity or availability of (personal) data unnoticed by the controller;

B. data being transferred to jurisdictions that do not provide adequate data protection;

C. acts in violation of laws and principles for privacy and data protection;

D. the controller accepting standard terms and conditions that give the cloud service provider too much leeway, including the possibility that the cloud service provider may process data in a way that contradicts the controller's instructions;

E. cloud service providers or their subcontractors using the controllers' data for their own purposes without the controllers' knowledge or permission;

F. accountability and responsibility seemingly fading or disappearing in a chain of subcontractors;

G. the controller losing control of the data and data processing;

H. the controller or its trusted third party (e.g. auditor) being unable to properly monitor the cloud service provider;

I. data protection authorities being precluded from properly supervising the processing of personal data by the controller and the cloud service provider; and

J. the controller relying on unfounded trust in the absence of insight and monitoring, thereby potentially contravening the data protection legislation in force in the country of establishment.

The following recommendations are intended to help **reduce risks associated with the use of cloud computing services and to promote accountability and proper governance**[6], so that the benefits of utilising CC can be achieved, but not at the expense of the rights of the individual.

Recommendations[7]

General recommendations

The Working Group recommends that:

- Cloud computing must not lead to a lowering of data protection standards as compared with conventional data processing;

- Data controllers carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on CC projects;

- Cloud service providers further develop their practices in order to offer greater transparency, security, accountability and trust in CC solutions in particular regarding information on potential data breaches and more balanced contractual clauses to promote data portability and data control by cloud users;

- Further efforts be put into research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC;

[6] On pages 9–10 of *Cloud Computing – Benefits, risks and recommendations for information security, November 2009*, ENISA lists the top security risks, in random order, as: loss of governance, lock-in, isolation failure, data protection, insecure or incomplete data deletion, malicious insider. For details see the publication. Loss of governance is emphasised here.

[7] The list of recommendations is not exhaustive.

- Legislators reassess the adequacy of existing legal frameworks allowing cross-border transfer of data and consider additional necessary privacy safeguards in the era of CC[8], and

- Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues.

Additional guidance on best practices

1. CC implementation should take place in careful, measured steps, starting with non-sensitive and non-confidential information.

2. The processing of sensitive[9] data via CC raises additional concerns. Therefore without prejudice to national laws such processing requires additional safeguards.

3. **Location audit trails** should be made available to controllers and DPAs. The audit trail should be recorded automatically and show the physical locations in which personal data have been stored or processed and when[10].

4. **An automatically recorded copying and deletion audit trail** should be established, showing clearly which copies of personal data the processor or its subcontractors have created and deleted.

5. The location audit trail and the copying and deletion audit trails should also include backup.

6. Effective **technical measures** should be developed against personal data illegally being transferred to jurisdictions without sufficient data protection.

7. It should be ensured that **deletion** of personal data from disks and other storage media can be executed in an effective way, e.g. through **immediate overwriting with random data**[11].

---

[8] Cf. International Conference of Data Protection and Privacy Commissioners: International Standards on the Protection of Personal Data and Privacy ("Madrid Resolution"), 5th November 2009; http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

[9] The concept of sensitive data carries different meanings in different legal cultures, cf. Art. 8 of Directive 95/46/EC, Art. 9 EU Draft General Data Protection Regulation and the FTC Report "Protecting Consumer Privacy in an Era of Rapid Change" (2012)

[10] E.g. the location audit trail could provide a clear overview of when the individual personal data are checked in and checked out at the individual locations, as well as when and to which location they are transferred.

[11] Deletion by dereference of data and later overwriting by reuse of the storage areas is generally not sufficient, as it opens the possibility that data become accessible again by renewed reference before or during the reuse of the storage areas.

8. It should be ensured that personal data at rest and in transit[12] are **encrypted** using recognised standard algorithms and contemporary key lengths. The encryption keys should not be used by, or be accessible to anyone other than the controller and cloud service provider. The encryption keys should not be used by, or be accessible to other customers of the cloud service provider. Data should not be available in unencrypted form longer and more extensively than is absolutely necessary for the data processing process at hand. Methods rendering data unreadable to CC providers at any given time should be further explored[13]. It could be useful to explore options by which the controller can effectively and quickly cut off the cloud service provider or its subcontractors from decrypting data (an emergency brake).

9. There should be automatic **logging** of all uses of personal data by cloud providers and their subcontractors. The log should be easily accessible to the controller and be designed in a simple, readily understandable form. The cloud service provider and its subcontractors should ensure the integrity of the logs.

Controller

10. In the agreement with the cloud service provider, the controller should secure a complete list of information in advance about all physical locations in which, throughout the duration of the agreement, data may be stored or processed by the cloud service provider and/or its subcontractors, including backup (**principle of location transparency**).

11. In the agreement, the controller should ensure that neither the cloud service provider nor its subcontractors transfer data to locations other than the physical locations listed in the contract, regardless of their reason for so doing, and regardless of whether the data are encrypted. This should be supported by technical measures whose existence and dependability the controller has an actual ability to inspect.

12. The controller should ensure that the agreement with the cloud service provider does not contain ambiguities or room for interpretations which undermine the principle that the cloud service provider only processes personal data according to the controller's instructions. Should cloud service providers

[12] For data in transit end-to-end encryption should be applied. It must be ensured that personal data in transit is protected against active (e.g. replays, traffic injection) and passive attacks (e.g. eavesdropping). Furthermore, access to data in rest by unauthorised parties must be prevented via corresponding technical and organizational mechanisms (e.g., access control, encryption of the data).

[13] An example of research in this area is the Sealed Cloud initiative, which is presented in the preprint paper Sealed Cloud – a novel approach to defend insider attacks by Hubert A. Jäger and Arnold Monitzer. The preprint is available from http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf

be able to unilaterally change the agreement the controller should have the right to terminate the contract and to transfer the data to a different cloud service provider.

13. The agreement should explicitly state that the cloud service provider may not use the controller's data for the cloud service provider's own purposes.

14. The controller should have the opportunity to inspect or have inspected all locations that process personal data wholly or partially in the present or have done so in the past, or may do so in the future under the agreement. The agreement should specify that the controller has the right to obtain full insight into all aspects of the cloud service provider and its subcontractors that the controller deems necessary to ensure compliance with the agreement, including ensuring that processing of personal data is done according to instructions, is done legally and in a suitably secure manner.

15. In the agreement, the controller should secure the right to let a trusted third party (e.g., a recognized auditing firm)[14] wholly or partially monitor the processing of personal data by the cloud service provider and its subcontractors, if any.

16. Prior to the use of CC, the controller should perform a **risk assessment** based on insight into the specific conditions and circumstances under which personal data will be processed by the cloud service provider and its subcontractors, if any. The risk assessment should include all of the locations at which personal data are processed or stored. If the cloud service provider uses subcontractors for parts of the processing, the risk assessment should also include all locations used by the subcontractors.

17. The controller should regularly review and update the risk assessment as long as personal data are processed by the cloud service provider.

18. Before use of CC, the controller should consider ensuring that there is a real exit option with the cloud service provider, including an active role in the transfer of data by the cloud service provider, in order not to become dependent on the cloud service provider (lock-in).

19. The controller should consider whether it is necessary to secure access to at least one usable copy of data outside of the cloud service provider's (and its subcontractors') control, reach or influence. If this is deemed necessary, the copy should be accessible and usable by the controller independently of the cloud service provider's and its subcontractors' participation.

[14] For more on trusted third parties, refer to section 44.

20. The controller should be able to fully fulfil its obligations towards data subjects and Data Protection Authorities in case of a **data breach** and take appropriate actions accordingly. As such, the controller should make clear agreements with the cloud service provider regarding a prompt and complete notification of the controller and/or Data Protection Authority in case of such a data breach.

21. The controller should contractually oblige the cloud service provider to implement effective and prompt procedures so that the data subjects can exercise their rights of access, rectification, erasure or blocking of data.

Cloud service provider

22. The cloud service provider should establish full transparency for the controller regarding the locations used for data processing and storage of personal data by the cloud service provider and its subcontractors, if any.

23. The cloud service provider should establish full transparency regarding the subcontractors used and what processing they perform for the cloud service provider.

24. The cloud service provider should provide transparency in contractual matters and refrain from offering CC on standard terms and conditions that allow for unilateral contract changes.

25. Cloud service provider and their subcontractors, if any, are encouraged to follow best practice and allow an impartial third party to conduct a comparison and assessment thereof (benchmarking).

26. Standard terms and conditions offered to certain market segments, e.g. small and medium enterprises should be drafted in such a way that respect of privacy and appropriate safeguards are taken into account.

Auditing

27. Given the possibility of very large accumulations of personal data by the cloud service provider, the cloud service provider should be subject to third-party audits in addition to the audit performed by the controller in the controller's own interest. The auditor should be fully independent of the cloud service provider and should pay special attention to the security aspects of processing of personal data. In particular, the auditor should check whether measures regarding the following are in place and functioning properly: location audit

trail (see section 3), copying and deletion audit trails (see section 4), deletion (see section 7), and logging (see section 9). Further, the auditor should check that the following are in place and functioning properly: measures to prevent the illegal transmission of data to jurisdictions with insufficient data protection (see section 6) and measures to prevent the transmission of data to other locations than those explicitly agreed with the customer (see sections 10 and 11). Lastly, the auditor should ensure that it is not possible for the cloud service provider or its subcontractors, if any, to circumvent these measures undetected.

Background for the recommendations

28. CC is a relatively **new paradigm** for data processing, evolving from what, for lack of a better term, is now being referred to as **traditional data processing**. Many years of solid experience with traditional data processing have accumulated, whereas there is no similar solid experience with CC.

29. The consequence of the **paradigm shift** is that basic assumptions, experiences, ideas, theories and models for data processing no longer correspond to the practice, and therefore must be subjected to critical reflection, reassessment and possible revision. This also applies to privacy and data protection of personal data and how **risks** can be analysed, assessed and judged. What was best practice yesterday is not necessarily best practice today.

30. The **new situation** must be examined and implemented with **carefully measured steps**, particularly with regard to privacy and data protection, and protection of the rights of the data subject in a wider sense.

31. The **technical foundation** of CC is well-developed network technology and virtualisation of servers. This enables quick dynamic relocation of data and data processing among servers locally in the individual cloud data centre and globally among cloud data centres in countries around the world. The technology is highly scalable without creating limiting bottlenecks. The internet allows the end user to access the data regardless of where the cloud data centres are located.

32. The **economic driving force** behind CC is **economics of scale**. Consolidating data processing in large centres improves the utilisation of expensive resources such as: human knowledge, tangible capital (HW, SW, buildings), communication bandwidth and energy. In addition, due to their size and volume, cloud service providers have significant bargaining power when purchasing resources. Cloud service providers can therefore reduce unit costs and offer attractive prices to customers. The prerequisite for achieving economics of

scale is many customers in "the store". To achieve sufficient **volume**, CC services are offered globally via the internet.

33. CC is considered to provide important opportunities for small and medium enterprises to have access to affordable and scalable computing resources. Due to the large number of relatively small entities, it is expected that cloud service providers will develop standard terms and conditions for this market segment.

34. CC is far more dynamic than traditional data processing. The location where data processing takes place can change dramatically. The current location of data and where it is processed can depend on a variety of factors to which end users and data controllers traditionally have given little thought, and into which they do not necessarily have the insight or ability to control. For example, cloud service providers often choose to locate their data centres across many countries and several continents, based on the availability of cheap electricity, a cool local climate and time zone differences, among other factors. Unpredictable circumstances can also impact the current location of data, such as interruptions in one data centre or a lack of capacity at peak periods (overflow). Copies of data can be transferred to other data centres to ensure online accessibility in case of interruptions in one data centre or for the purpose of making backups (redundancy).

35. CC is based on many cloud customers dynamically sharing a common pool of the cloud service provider's resources. This should only take place if it is possible to maintain **robust separation** of the different cloud customers' data and their processing. Resource sharing entails an increased risk of large scale losses or unauthorised disclosure of data.[15] The risk is further enhanced by the fact that CC is driven by cost optimisation based on high volume (economics of scale). Cloud customers constitute a risk to each other. The more customers sharing the same resources, the greater the risk for each individual customer, and thus for cloud customers as a whole.

36. Knowledge about CC and insight into its risks are currently concentrated among relatively few large cloud service providers, who for commercial and competitive reasons appear to be reluctant to give the world insight into specific conditions and circumstances. The uneven distribution of knowledge and insight between cloud service providers and customers places the latter in a weak position when entering into agreements and makes it difficult for them to properly assess risks associated with the intended use of CC.

[15] On pages 9-10 of *Cloud Computing – Benefits, risks and recommendations for information security, November 2009*, ENISA lists the top security risks, in random order, as: loss of governance, lock-in, isolation failure, data protection, insecure or incomplete data deletion and malicious insider. For further details, refer to the publication; here it should be emphasised that isolation failure is considered a top risk.

37. A thorough **risk assessment** must be based on **insight** into the concrete setup and circumstances of the cloud service provided at all of the locations where data processing will take place.

38. CC technology is **boundless** and **transboundary**. The global customer base, in tandem with the global distribution of cloud data centres and dynamic movement of data (and data processing), can result in data crossing national borders and changing jurisdictions with a corresponding lack of transparency. Personal data may end up in data centres in jurisdictions with inadequate data protection or personal data may be misused commercially or be accessed without authorisation by foreign powers[16].

39. A distinction must be made between the two mutually exclusive roles of controller and processor within data protection. The **controller** is the one who determines the purpose and means used for a specific act of data processing.

40. It is also widely acknowledged that a controller may allow the processing of personal data to be performed by a **processor** but only in accordance with the controller's explicit **instructions**.

41. A commonly recognised data protection principle is that the processor must not process personal data to a greater extent than that which follows from the explicit instructions from the controller.[17] For CC, this implies that a cloud service provider cannot unilaterally make a decision or arrange for personal data (and its processing) to be transmitted more or less automatically to unknown cloud data centres. This is true whether the cloud service provider justifies such a transfer as a reduction of operating costs, management of peak loads (overflow), load balancing, copying to backup, etc. Nor may the cloud service provider use personal data for his own purposes.[18]

42. Another generally recognised data protection principle requires that the controller implement appropriate **technical and organisational security measures** to protect data against accidental or unlawful destruction, loss or deterioration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down by the law. The same applies for processors.

[16] Whilst personal data may be processed within one jurisdiction, the cloud provider, or parent company, may also be established within another jurisdiction thereby allowing foreign law enforcement powers access to the data within the cloud service even though that data physically resides outside the geographical boundaries of that country. An international agreement may be required to address this issue.

[17] Or by legislation.

[18] If cloud service providers process data without the knowledge of the controller, the cloud service provider should be seen as a co-controller and as such be held accountable for the unauthorised independent processing of data.

43. Fulfilment of the controller's responsibility requires that the controller **monitor** the processing by the processor to ensure that it takes place according to the controller's instructions and that the processing is done with adequate security.

44. Without removing his liability, the controller can give explicit instructions that monitoring of processing by the processor be partially performed by a **trusted third party** (e.g. auditor). The prerequisite is that the third party has the necessary qualifications, is independent of the processor, has full access to and insight into the actual conditions and circumstances under which processing by the processor takes place and can reliably report his observations, assessments and conclusions to the controller.

The Working Group will continue to monitor developments in the area of cloud computing and update this paper as necessary.

2013

53. Sitzung, 15. und 16. April 2013, Prag, Tschechische Republik

Arbeitspapier

Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar

Einleitung

1. Dieses Papier gründet auf der Achtung der Grundrechte und Grundfreiheiten der Internetnutzer. Obgleich der Fokus nicht auf besonderen technischen Maßnahmen liegt, geht das Papier gleichwohl davon aus, dass das technische Verfahren des Webtracking rechtmäßig und angemessen sein und dass es sich innerhalb eines strengen Rahmens dieser Rechte bewegen muss. Die Grundsätze von Wahlmöglichkeiten und Kontrolle – die von großen Teilen der Wirtschaft gefordert werden – bilden das Zentrum dieses Rahmens; diese Grundsätze müssen mit Genauigkeit auf den Säulen von Klarheit, Transparenz und Verantwortlichkeit

umgesetzt werden. Die Rechtfertigung für die Durchführung von Webtracking ist nicht offenkundig, deshalb müssen die Wirtschaft und andere Vertreter, die Tracking durchführen, beständig nach Lösungen suchen, die diese Tätigkeit nicht nur voll und ganz in den Rahmen der Grundrechte und Privatsphäre einpassen, sondern sie auch mit dem Gebot des „Privacy by Design" *[Einbeziehung des Schutzes der Privatsphäre schon bei der Entwicklung von Technologien]* in Einklang bringen.

2. In diesem Arbeitspapier behandelt die Arbeitsgruppe das Thema Webtracking und Privatsphäre. Obgleich es keine klare Definition dafür gibt, werden wir uns auf eine Definition des Webtracking[1] beziehen, nämlich als der Erhebung, Analyse und Anwendung von Daten über Nutzeraktivitäten von einem Computer oder Gerät aus, wenn verschiedene Dienste der Informationsgesellschaft (nachfolgend: das Internet)[2] genutzt werden, um diese Nutzungsdaten zu verschiedenen Zwecken zusammen zu führen und zu analysieren, und zwar von wohltätigen und philantropischen bis hin zu kommerziellen Zwecken. Wir sind der Meinung, dass verschiedene Formen der Marktforschung unter diese Definition des Webtracking fallen, zum Beispiel die Reichweitenmessung („outreach measurement" – der Umfang, in dem Nutzer Anzeigen überall im Internet angezeigt bekommen), das Messen des Nutzungsverhaltens („engagement measurement" – der Umfang, in dem Nutzer mit Internetdiensten in Interaktion treten) und das Messen der erreichten Nutzer („audience measurement" – der Umfang, in dem Mikroprofile der Nutzer aus ihrer Interaktion mit Angeboten im Internet abgeleitet werden können).[3]

Umfang des Arbeitspapiers

3. Dieses Papier richtet sich an alle Anbieter von Web-Sites sowie an Softwareentwickler und Service Provider *[Diensteanbieter]*, die Trackingtechnologien anbieten oder nutzen. Dieses Papier diskutiert die Entwicklung von Trackingtechnologien und ihre möglichen Auswirkungen auf die Privatsphäre der Bürgerinnen und

[1] van Eijk (2012), The DNA of OBA: unique identifiers [Die DNA der OBA: Eindeutige Identifikatoren] [OBA = Online Behavioural Advertising = Online-Werbung mit Nutzung des Surfverhaltens der Nutzer], URL: http://www.campusdenhaag.nl/crk/publicaties/robvaneijk.html#definition-of-web-tracking.

[2] Beachten Sie bitte, dass dadurch, dass die Technologie auf IP-Grundlage zunehmend zum Rückgrat der Informationsgesellschaft wird und viele andere früher eigenständige Technologien integriert wurden („Konvergenz"), dies auch die Nutzung von Telefon (IP-Telefonie) und Fernsehen (IPTV), das Lesen digitaler Zeitungen oder jeglicher anderer Medienkonsum mittels digitaler Technologien (einschließlich das Lesen eines E-Buches) mit umfassen kann. Zu einer detaillierten Diskussion der sich daraus ergebenden Gefahren für die Privatsphäre siehe das Working Paper „Privacy Issues in the Distribution of Digital Media Content and Digital Television *[Arbeitspapier zu Themen der Privatsphäre bei der Verbreitung digitaler Medieninhalte und des digitalen Fernsehens]* (Berlin, 4./5.09.2007) dieser Gruppe; URL: http://www.datenschutz-berlin.de/attachments/349/digit_de.pdf.

[3] JICWEBS Reporting Standards *[Grundsätze der Berichterstattung im Internet des Joint Industry Committee for Webstandards]*, URL: http://www.abc.org.uk/PageFiles/50/Web Traffic Audit Rules and Guidance Notes version2 March 2013 master.pdf.

Bürger. Es befasst sich mit digitalen Spuren, die wir hinterlassen, wenn wir die verschiedenen Dienste der Informationsgesellschaft mit einem Webbrowser nutzen, dazu gehören auch eindeutige Identifikatoren („unique identifier"), die mit Hilfe von Technologien erlangt werden, die ohne Cookies arbeiten.[4] Dazu zählen ferner auch Webbrowser auf anderen Geräten, zum Beispiel auf Smartphones und Smart-TV-Geräten.

4. Dieses Papier befasst sich nicht mit besonderen zusätzlichen Gefahren der Nutzung von Apps auf mobilen Geräten.[5] Nichtsdestotrotz sollten die Grundsätze dieses Papiers ebenso auf in anderen Diensten eingesetzte Trackingmethoden angewandt werden.

5. In diesem Papier geht es nicht darum, wie Schutzmaßnahmen umgesetzt werden können (z. B. rechtliche Anforderungen an eine Einwilligung). Anzumerken ist jedoch, dass in manchen Rechtsordnungen zwar je nach Zweck des Webtracking, die ausdrückliche Einwilligung (Opt-in) erforderlich ist, in anderen Rechtsordnungen jedoch die Möglichkeit zum Widerspruch („Opt-Out") für das Webtracking als gültig betrachtet wird, um den Anforderungen des Rechtssystems zu genügen, wenn bestimmte Bedingungen erfüllt sind. Diese umfassen unter anderem die angemessene Benachrichtigung über die Verarbeitung von Daten; Transparenz in der Benachrichtigung; Benachrichtigung zum Zeitpunkt der Sammlung der Daten oder zuvor; und einfache, wirksame und dauerhafte Möglichkeiten zum Widerspruch. Eine Reihe von Beschränkungen kann ebenso vorhanden sein; z. B. in Bezug auf die Verarbeitung sensibler Informationen wie zum Beispiel Informationen über die Gesundheit, über politische oder weltanschauliche Ansichten und die Verhinderung des Tracking von Kindern.

Hintergrund

6. Die technischen Möglichkeiten für die Beobachtung der Aktivitäten der Nutzer auf Web-Sites haben sich in den letzten zehn Jahren vervielfältigt; die „Informationsgesellschaft" hat seitdem schon mehrere grundlegende Veränderungen erfahren.[6] Webtracking entwickelte sich aus sehr bescheidenen Anfängen – als einzelne Provider von Online-Diensten mit der Beobachtung ihrer Nutzer mit dem Ziel der Feststellung begannen, ob ein bestimmter Nutzer diese Web-Site

[4] Zum Beispiel die passive Fingerprinting-Technik, die auf dem Hashing des HTTP Endsystemteils bzw. der IP-Adresse des Ursprungs-Browsers basiert.

[5] Siehe zum Beispiel die von der Artikel-29-Datenschutzgruppe (Art. 29 WP) herausgegebene Stellungnahme 02/2013 über Apps auf Smart-Geräten WP 202, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

[6] Die Literaturübersicht über die Messung der Privatsphäre im Internet, welche als Ergebnis der Konferenz zur Messung der Privatsphäre im Internet (Conference on Web Privacy Measurement, WPM) zusammengestellt wurde, gibt einen ausführlicheren Überblick über die für das Tracking eingesetzten Technologien, URL: http://www.law.berkeley.edu/12633.htm.

schon zuvor besucht hatte und was dieser Nutzer dort getan hatte – in jüngerer Zeit zu einer schon fast bizarren Vision der Anbieter. In dieser Vision scheint der Anbieter in der Lage zu sein, jeden einzelnen Aspekt des Verhaltens eines erkennbaren Nutzers im gesamten Internet zu beobachten. Dies könnte eine vollständige Verlaufsübersicht über die umfassende Nutzung des Internets einer betroffenen Person über unbegrenzte Zeitspannen hinweg (wortwörtlich von der Wiege bis zum Grab) werden, und diese *[Verlaufsübersicht]* könnte mit Profildaten aus der „Offline-Welt" angereichert werden (einschließlich aller möglichen Aspekte aus unserem Leben, über die die Datenmakler Informationen besitzen; dazu gehören auch Informationen über Finanzen sowie Informationen über zum Beispiel Freizeitgestaltung, Gesundheit, politische bzw. religiöse Überzeugungen und Informationen über Aufenthaltsorte).[7]

7. Diese Entwicklung – die zwar von Anbietern und anderen Interessenten in der Geschäftswelt begrüßt und gefördert und von einigen Politikern auf nationaler und regionaler Ebene unterstützt wird – birgt eine beispiellose Gefahr für die Privatsphäre aller Bürger in der Informationsgesellschaft. Sie könnte schlimmstenfalls die uns bekannte Welt zu einem globalen Panoptikum wandeln: Das Offline-Äquivalent wäre, wenn uns ein Unbekannter ständig über die Schulter schauen würde, ganz gleich, wo wir uns befinden (auf der Straße oder in der scheinbaren Privatsphäre zu Hause) – oder was wir gerade tun (fernsehen, online einkaufen, Zeitung lesen und sogar noch intimere Tätigkeiten) und ohne dass wir wissen, wann der Unbekannte gerade zuschaut und wann nicht.[8]

8. Die möglichen Auswirkungen einer solchen Entwicklung liegen auf der Hand und sind im Hinblick auf ihre mögliche Schwere nicht zu unterschätzen: Sie kann einige der wesentlichen Grundsätze der Privatsphäre aufheben oder anullieren, – und insbesondere *[die Grundsätze von]* Transparenz und Kontrolle durch die Bürgerinnen und Bürger.[9] Um es noch deutlicher zu sagen: Dies könnte das Ende der Welt (in Bezug auf den Schutz der Privatsphäre) sein, wie wir sie kennen.

9. Die Befürworter dieser Vision behaupten andererseits, dass diese Gefahren entweder gar nicht vorhanden sind oder dass sie versucht haben, sich mit diesen Gefahren zu befassen und sie zumindest zum Teil abzuschwächen: Es gibt einen starken Widerstand seitens mancher Interessenvertreter der Wirtschaft dagegen, anzuerkennen, dass eindeutige Identifikatoren Daten über die Internetnutzung personenbezogene Informationen sind. Eine oftmals vorgebrachte Behauptung

[7] In Systemen zur Pflege der Kundenbeziehungen (Customer Ralationship Management, CRM) sind hierfür die üblichen Begriffe Customer Lifetime *[Kundenleben]* und Customer Lifetime Value *[Kundenkapitalwert]*.

[8] Und um die Dinge noch zu verschlimmern, würde diese modernistische Version eines Panoptikums jede einzelne Bewegung einer jeglichen Privatperson und zu einem jeden Augenblick aufzeichnen, unabhängig davon, ob der Wächter gerade hinschaut oder nicht.

[9] Tracking als Technologie ist nicht transparent: Auf technischer Ebene sind in vielen Fällen die Pixel *[Bildpunkte]* (z. B. Web-Beacons *[Code-Fragmente]*) und Mini-Web-Sites (z. B. iFrames) für das menschliche Auge unsichtbar.

ist, dass bei vielen der genutzten Daten die Rückverfolgung auf eine bestimmte Person nicht mehr möglich ist (d. h. die Daten anonymisiert wurden) und dass, sobald dieses erledigt ist, die Daten sich nicht mehr auf eine Person beziehen und deshalb keine Gefahr mehr für die Privatsphäre von Bürgern darstellen würden. Auch wird vorgebracht, dass alle Daten über Verhaltensweisen nur mit Maschinen verbunden sind und – dies ist die Behauptung – in sehr vielen Fällen überhaupt nicht zu einer bestimmten Person zurückverfolgt werden können.

10. Allerdings gibt es für diese Behauptungen keinerlei wissenschaftlichen Nachweis und sie lassen die Tatsache außer Acht, dass Maschinen – und insbesondere Smartphones – zunehmend zu persönlichen Geräten werden und eine Verbindung zu einem jeden individuellen Nutzer leicht ermöglichen. Spuren können auch in zunehmendem Maße über verschiedene Geräten hinweg verbunden werden. Ebenso gibt es einen wissenschaftlichen Nachweis dafür, dass viele anscheinend anonyme Daten (z. B. Informationen über den Aufenthaltsort bei Mobiltelefonen) zu dem betroffenen Nutzer zurückverfolgt werden können (d. h. ihre Anonymisierung wird aufgehoben), wenn die Datenbasis und der zeitliche Rahmen groß genug sind. Jüngere wissenschaftliche Arbeiten lassen sogar vermuten, dass es grundsätzlich unmöglich ist, „anonyme" Daten vor einer Deanonymisierung zu schützen, wenn der Zeitintervall für die Beschreibung eines beliebigen Verhaltens groß genug ist (d. h. es ist schon konzeptuell unmöglich, zu garantieren, dass „anonyme" Daten im Laufe der Zeit nicht zu einer bestimmte Person zurückverfolgt werden können). Wenn dies richtig ist, stellt es eine bahnbrechende Entwicklung dar und würde eine Reihe von Kernannahmen darüber, wie sich die Nutzung verschiedener Arten von Daten auf die Privatsphäre von Personen auswirken kann oder nicht, sinnlos machen.[10]

11. Darüber hinaus und mit leicht anderer Ausrichtung trägt auch die praktische Erfahrung des Alltags dazu bei, die von der Industrie aufgestellten Behauptungen in Frage zu stellen: Werbeanzeigen werden zwar auf technischer Ebene an eine Maschine gerichtet, es ist aber nicht die Maschine, die letzten Endes die sprichwörtlichen „schönen roten Schuhe" kauft – es ist der oder die Einzelperson. Deshalb kann die Behauptung, dass die Verarbeitung von Daten über Verhaltensweisen für Marketingzwecke sich „nur" zunächst an Maschinen richtet, sehr wohl als ein Versuch betrachtet werden, unseren Blick als Gesellschaft insgesamt hinsichtlich der Ernsthaftigkeit des Problems zu trüben, da in der Realität der Mensch und nicht die Maschine die einzige Instanz ist, die alle solche Trackingoperation zu einem „Erfolg" für die Befürworter gestalten kann (d. h., wenn die roten Schuhe schließlich gekauft werden).

[10] Cf. Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization *[Gebrochene Versprechen zur Privatsphäre: Eine Antwort auf das überraschende Versagen der Anonymisierung]*, August 2009. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

Eine kurze Geschichte der Technologien für Beobachtungszwecke

12. Bei dem Versuch, die oben beschriebene Entwicklung bis zu ihren bescheidenen Anfängen hin zurück zu verfolgen, stellt die Entwicklung der „Cookie-Technologie" vor fast 20 Jahren ein Meilenstein dar: HTTP-Cookies wurden 1994 eingeführt, und zwar in erster Linie, um das „kleine" Problem der verlässlichen Umsetzung eines virtuellen Einkaufswagens zu lösen. Weil das Hypertext Transfer Protocol (HTTP) überwiegend zustandslos („stateless") war, konnten Endsysteme bis zu diesem Zeitpunkt keine Zustandsinformationen speichern. Die Speicherung von Zustandsinformationen war jedoch für den virtuellen Einkaufswagen ganz wesentlich, um ausgewählte Artikel beim Shopping-Vorgang zu speichern. Transparenz war schon zu diesem Zeitpunkt ein Thema im Hinblick auf die Privatsphäre, weil die Verwendung von Cookies dem gewöhnlichen Nutzer nicht mitgeteilt wurde. Zu jener Zeit wurden Cookies standardmäßig in den Browsereinstellungen freigegeben und der Nutzer wurde über den Einsatz von Cookies nicht informiert.[11]

13. Um Gefahren für die Privatsphäre und die Sicherheit zu entschärfen, die sich daraus ergeben, dass Cookie-Informationen ungewollt zu Betreibern anderer Web-Sites gelangen, wurde die Same-Origin-Policy *[Grundregel desselben Ursprungs, SOP]* eingeführt. Diese Maßnahme bedeutet, dass Cookies nur von derselben Domain gelesen werden konnten, die sie gesetzt hat. Allerdings muss darauf hingewiesen werden, dass das World Wide Web Consortium (W3C) *[Gremium zur Standardisierung der das Internet betreffenden Techniken]* einen neuen Standard vorgeschlagen hat, nämlich das Cross Origin Resource Sharing (CORS)[12], welches den Informationsaustausch domainübergreifend zulässt. Obgleich CORS ein freiwilliger Standard ist, steht er im Widerspruch zur Same-Origin-Policy.

14. Bereits 1998 befasste sich diese Gruppe[13] mit verschiedenen Fragestellungen zur Privatsphäre in Verbindung mit der systematischen Sammlung oder Nutzung personenbezogener Daten im Internet.[14] In dem Arbeitspapier beschäftigte sie sich mit P3P (Platform for Privacy Preferences Project) *[Plattform zum Austausch von Datenschutzinformationen]*, einem vom W3C entwickelten Protokoll, welches darauf ausgelegt war, Cookies von Dritten zu blockieren, es sei denn, dass die vom Nutzer besuchte Web-Site eine für den Nutzer akzeptable P3P-Policy *[P3P-*

[11] RFC 2109, HTTP State Management Mechanism, URL: https://tools.ietf.org/html/rfc2109. Beachten Sie, dass aktuelle Varianten der Speichertechnik für Cookies zum Beispiel auch Flash-Cookies und LSOs (Local Shared Objects) umfassen, die in HTML5 mit entsprechenden Werten verwendet werden.

[12] Cross-Origin Resource Sharing, URL: http://www.w3.org/TR/cors/ (abgerufen am 30. Mai 2013).

[13] International Working Group on Data Protection in Telecommunications *[IWGDPT,Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation]*.

[14] Gemeinsamer Standpunkt zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien (z. B. P3P) im WorldWideWeb; (Hong Kong, 15.04.1998), http://www.datenschutz-berlin.de/attachments/177/priv_de.pdf

Datenschutzrichtlinie] anbot.[15] Allerdings hat nur ein großer Browserhersteller den Standard umgesetzt. Infolgedessen wurde P3P in keinem breiten Umfang im Internet angenommen.

15. Third Party Cookies *[Cookies von Dritten]* sind zum Lebensnerv der komplexen digitalen Werbeindustrie geworden. 2008 diskutierten leitende Marketingfachleute aus Webtracking-Unternehmen die Zukunft von Webanalyse und Webstatistik. Die Zukunft in fünf Jahren stellte man sich so vor, dass die traditionelle Webstatistik über die Besuche der Web-Site (nachfolgend: First und Third Party Analytics) mit Analysedaten anderer Webanalysedienste zusammengeführt wird, zu denen auch zum Beispiel Videodienste, Widgets *[Komponenten von Benutzeroberflächen]*, soziale Netzwerke, Spiele und Suchmaschinen gehören (nachfolgend: Web Analytics).[16]

16. Heutzutage stellen Daten aus Webanalysen eine neue Form des wirtschaftlichen Wertes dar. Zwar stellt diese Gruppe nicht den Nutzen in Frage, den das Messen des Verbraucherverhaltens für das Online Behavioural Advertising (OBA) *[Online-Werbung mit Nutzung des Surfverhaltens der Nutzer]* (in Echtzeit) bringen kann, doch ist sie der festen Überzeugung, dass solche Methoden nicht auf Kosten der Rechte von Privatpersonen im Hinblick auf Privatsphäre und Datenschutz eingesetzt werden dürfen.

Webtracking

17. Das Webtracking umfasst die Erhebung und nachfolgende Speicherung, Nutzung oder den Austausch von Daten des individuellen Online-Verhaltens über eine Vielzahl von Web-Sites durch den Einsatz von Cookies, JavaScript oder jeglichen anderen Formen des Device Fingerprinting *[Ermittlung von Einzelpersonen anhand von Eigenschaften technischer Geräte, z. B. Browser-Einstellungen]*. Webtracking-Technologien ermöglichen einen konstanten Fluss von Informationen über Nutzer in Echtzeit, wie zum Beispiel Registrierungsdaten, Daten über die Online-Suche, verhaltensbezogene Daten, Statistiken über Besuche von Web-Sites und Conversion-Daten *[Daten über Umwandlung von Klicks in Handlungen, wie z. B. Einkäufe]*, die alle widerspiegeln, auf welche Art und Weise ein Nutzer auf individuelle Angebote reagiert hat. Diese Daten können genutzt werden, um

[15] Das Platform for Privacy Preferences Project (P3P) ermöglicht Web-Sites, ihre jeweiligen Methoden für den Umgang mit Privatsphäre in einem Standardformat auszudrücken, das automatisch abgefragt und von Nutzeragenten *[Anwendungssoftware, z. B. browser]* leicht interpretiert werden kann. P3P Nutzeragenten ermöglichen den Nutzern, über Methoden der Web-Site Kenntnis zu erlangen (sowohl in maschinenlesbaren, als auch für Menschen lesbaren Formaten) und Entscheidungsprozesse gegebenenfalls auf der Grundlage dieser Methoden zu automatisieren. Nutzer müssen nicht auf jeder von ihnen besuchten Web-Site die Datenschutzrichtlinien lesen. URL: http://www.w3.org/P3P/.

[16] Omma Global Measurement 3.0, http://www.webmetricsguru.com/archives/2008/09/measurement-30-on-the- next-5-years-omma-global-day-2/.

auf die Interessen, politischen Überzeugungen oder Krankheiten eines Nutzers zu schließen. Sie können mit dem Ziel verarbeitet werden, den Zustand oder das Verhalten einer bestimmten Person einzuschätzen, beides auf eine bestimmte Art und Weise zu behandeln oder zu beeinflussen. Daten über individuelles Verhalten lenken geschäftliche Entscheidungen auf der Grundlage von Kundenprofilen. Eine Kaufabsicht kann aus der vermuteten digitalen Identität einer Person abgeleitet werden. Der Wert eines potenziellen Kunden wird mit der Möglichkeit in Verbindung gebracht, ihn zum Kauf einer Ware zu bringen.

18. Webtracking-Technologie ist auf mobilen Geräten vorhanden. Privatpersonen tauschen ein mobiles, „smartes" Gerät untereinander sehr wahrscheinlich nicht aus, und daher ist die Verbindung zwischen dem Gerät und der Privatperson enger als zum Beispiel zwischen Mensch und Desktop-Computer. Mobile Geräte enthalten eindeutige Geräte-Identifikatoren, wie zum Beispiel besondere Identifikatoren für Werbung,[17] die Unique Device ID (UDID) *[eindeutige maschinenlesbare Kennung]*, die MAC-Adresse (Media Access Control) *[Hardware-Adresse z. B. jedes einzelnen Netzwerkadapters]*, die Bluetooth MAC-Adresse, die NFC MAC-Adresse (Near Field Communications) *[international genormter Standard zur Datenübertragung im Nahbereich]*, die International Mobile Subscriber Identifier (IMSI, eine eindeutige SIM-Kartennummer) und die International Mobile Equipment Identifier (IMEI) *[eindeutige Seriennummer bei Mobilgeräten]*. Diese Identifikatoren kann der gewöhnliche Nutzer nicht ändern. Über eindeutige Identifikatoren hinaus können mobile, „smarte" Geräte eine große Menge an Daten enthalten, wie zum Beispiel Nutzernamen, Passwort, Alter, Geschlecht und das Adressbuch. Solche Geräte können genaue verhaltensbezogene Daten über den Aufenthaltsort eines Nutzers offenlegen. Präzise Geopositionsdaten stehen für Browser auf mobilen, „smarten" Geräten fertig nutzbar zur Verfügung.

19. Webtracking-Technologie wird auf verschiedene Art und Weise eingesetzt. Eine digitale Datenspur kann sich aus der unabsichtlichen oder ungewollten Offenlegung von Daten ergeben und zu einer nicht erforderlichen Offenlegung (personenbezogener) Daten führen. Es gibt sehr viele verschiedene Wege zur Erzeugung einer digitalen Datenspur. Zum Beispiel könnte der Manager einer digitalen Anzeigenaktion dem Nutzer, Browser oder Gerät einen eindeutigen Identifikator zuordnen. Ein anderer Weg ist die Personalisierung von Verweisinformationen durch Hinzufügen von Zielgruppeninformationen (Mikroprofile) beim Surfen im Internet, sodass andere Web-Sites, die sich auch an der Werbeaktion beteiligen, den Nutzer, Browser oder das Gerät ebenso nachverfolgen können. Ein drittes Beispiel ist die Korrelation eindeutiger Identifikatoren mit aus früheren Besuchen auf einer bestimmten Web-Site gesammelten Daten. Und ein viertes Beispiel ist, dass Webtracking für eine Werbeaktion durch die Kombination neuer Tracking-

[17] Um zum Beispiel Frequency Capping durchführen zu können (Kontrolle der Häufigkeit, wie oft einem Nutzer eine Anzeige von Online-Werbung eingeblendet wird), Behavioral Ads *[auf Surfverhalten beruhende Anzeigen]* einzublenden und die Reichweite und Wirksamkeit einer Werbeaktion zu messen.

daten (über einen Nutzer, einen Browser oder Gerätedaten) mit zuvor auf einer bestimmten Web-Site gesammelten Daten oder mit von einem anderen oder Dritten erhaltenen Daten stattfinden kann. Ein letztes Beispiel sieht die Nutzung von Cookie Matching-Services *[Dienste zum Abgleich von Cookies auf besuchten Web-Sites mit dem auf dem Computer des Nutzers abgelegten Cookie]* vor, welche digitale Spuren desselben Nutzers, Browsers oder Gerätes mit der Nutzung verschiedener Teile des Internets verbinden.[18]

20. Webtracking besteht aus mehreren automatisierten Schritten, beginnend mit der Erhebung von Daten über die Internet-Nutzung, der Speicherung dieser Daten und der Nutzung der Daten. Durch neue Zusammenstellung der Daten, Korrelation und ihre Dekontextualisierung können Internetdaten dazu genutzt werden, sehr detailgenaue Profile und Vorhersagen individuellen Verhaltens aufzubauen. Schließlich führt das Webtracking zur tatsächlichen Anwendung des Profils einer bestimmten Person.

21. Daten können mittels verschiedener Dienste im Internet in einer Graphen-Datenbank gespeichert werden.[19] Die Struktur des Graphen ermöglicht die Herausbildung von Verhaltensmustern, die sonst unentdeckt geblieben wären. Webtracking-Daten in einem Graphen können aus sich selbst heraus oder durch Kombination mit anderen Daten aus verschiedenen Quellen aussagekräftige Muster über das Nutzerverhalten generieren. Zum Beispiel geben einzelne eindeutige Identifikatoren, die direkt oder indirekt mit einem Nutzer oder Computer verbunden sind, zwar nur wenige Informationen über den gelegentlichen Surfer bekannt, doch die Sammlung eindeutiger Identifikatoren bietet einen tief greifenden Einblick in die Gewohnheiten und das Surfverhalten einer Person im Internet. Die Sammlung eindeutiger Identifikatoren kann zur Erstellung einer digitalen Identität benutzt werden.

Webtracking und das Recht auf Privatsphäre und Datenschutz der Privatperson

22. Ein Schlüsselgrundsatz für eine große Bandbreite internationaler Rechtsordnungen ist das Recht auf Privatsphäre, das der Internetnutzer unabhängig von der Technologie besitzt. Schlüsselelemente sind Transparenz, Kontrolle und Beachtung des Kontextes. Es ist eine Gefahr für die Privatsphäre, dass Nutzern nicht bewusst ist, dass ihre Spuren verfolgt werden. Webtracking als Prozess verwendet eine Reihe technischer Tools, die die Gelegenheit der Mitteilung an die Nutzer

[18] Siehe zum Beispiel URL: https://developers.google.com/ad-exchange/rtb/cookie-guide#what-is.

[19] Ein Graph basiert auf der Graphentheorie, die einen mathematischen Ansatz für die Entwicklung paarweiser Beziehungen zwischen Objekten darstellt. Eine Graphdatenbank speichert Graphen, welche im wesentlichen Strukturen mit Knoten, Ecken und Eigenschaften darstellen. Die Eigenschaften können Metainformationen über die Knoten und Ecken enthalten.

begrenzen. Zum Beispiel sind Pixel (z. B. Web-Beacons) und Mini-Web-Sites (z. B. iFrames) für das menschliche Auge unsichtbar und ihre Einbindung in eine Web-Site löst eine automatische HTTP-Anfrage einschließlich der Möglichkeit des Setzens von und des Zugangs zu Cookies aus, die ihrerseits eindeutige Identifikatoren enthalten.

23. Viele Webtracking-Technologien wurden entwickelt und in der Wirtschaft eingesetzt, ohne dass den Nutzern Informationen darüber bereitgestellt wurden, wessen Daten gesammelt werden und ohne ihnen eine Wahlmöglichkeit zu bieten. Meldungen des Nutzers, die als Ausdruck der Ablehnung des Tracking verstanden werden könnten, wurden nicht beachtet und technische Methoden gegen einige Trackingmethoden wurden aktiv umgangen, zum Beispiel durch erneutes Hervorbringen gelöschter Cookies, (passives) Fingerprinting und das Umgehen von Browsereinstellungen. Erst als dieses Verhalten aufgedeckt und öffentlich kritisiert wurde, haben die entsprechenden Parteien ihre Verpflichtung akzeptiert, den freien Willen des Nutzers zu achten. In solchen Fällen wurden manchmal Opt-Out-Programme hinzugefügt, was aber oft zu schwerfälligen Mechanismen mit nur begrenztem Nutzen für den Nutzer führte. Diese Fälle haben im Hinblick auf das Vertrauen der Nutzer in die Verlässlichkeit und Aufrichtigkeit aller Internetanbieter einen großen Schaden verursacht und die gesunde Entwicklung innovativer Internetdienste untergraben.

24. Webtracking bedeutet in vielen Rechtsordnungen die Verarbeitung personenbezogener Daten, und zwar aufgrund der Tatsache, dass die Technologie die Individualisierung oder Identifizierung[20] von Nutzern bzw. das Treffen automatisierter Entscheidungen über sie ermöglicht. Ein Beispiel einer solchen Praxis könnten Maschinen für automatische Entscheidungen mit Algorithmen in Real Time Bidding Plattformen *[Verfahren für Werbungtreibende für das Bieten auf Werbeplätze in der Online-Werbung in Echtzeit]* für personalisierte Werbung auf der Grundlage von Nutzerverhalten sein.

25. Es gibt einen starken Widerstand seitens einiger beteiligter Interessengruppen gegen die Einstufung eindeutiger Identifikatoren in Webdaten als personenbezogene Informationen. Eine oftmals vorgebrachte Behauptung ist die, dass sobald Daten anonymisiert wurden,[21] diese Daten nicht mehr personenbezogen sind. Es sollte jedoch klar sein, dass auch ein „zweckgebundenes" Element dafür

[20] Erwägungsgrund Nr. 26 der allgemeinen Datenschutzrichtlinie 95/46/EG: Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html] (…), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[21] De-Identifikation von Daten einer bestimmten Person bedeutet das Entfernen, Ändern, Kumulieren, Anonymisieren oder anderweitige Manipulation von Daten.

verantwortlich sein kann, dass Informationen „sich“ auf eine bestimmte Person „beziehen“ oder diese Person betreffen können.[22]

Die potenzielle Wirkung (oder mangelnde Wirkung) des „Do Not Track“ (DNT) *[nicht verfolgen]* – eine Fallstudie

26. Im September 2011 gründete das W3C die Tracking Protection Working Group[23] *[Arbeitsgruppe zum Schutz vor Webtracking]*. Die Gruppe arbeitet an einem Do-Not-Track Standard (DNT). Alle großen Browserhersteller haben sich zwar dazu verpflichtet, den Standard umzusetzen (und die meisten haben bereits den HTTP-Header umgesetzt), allerdings dauert bei jenen Interessengruppen, die den DNT:1 Request[24] beachten werden, eine offene Diskussion über Teile des freiwilligen Standards an. Einige Interessengruppen haben angedeutet, das DNT-Flag aus verschiedenen Gründen nicht beachten zu wollen. Der übergreifende Erfolg von DNT ist von der tatsächlichen Beachtung des DNT-Flag durch die empfangende Organisationen und der tatsächlichen Annahme des DNT-Standards im gesamten Internet durch alle Interessengruppen abhängig.

27. Standardeinstellungen im DNT und die Standardaktionen der Webtracking-Organisationen bleiben wiederum äußerst wichtig. Damit DNT ein wirksames Instrument für die Umsetzung der Kontrolle durch den Benutzer ist, ist es somit äußerst wichtig, dass die Betreiber von Webtracking auch sicher sein können, dass die von ihnen empfangene DNT-Meldung eine echte Anzeige der Wünsche des Nutzers darstellt. Fehlt dem Nutzer eine solche Wahlmöglichkeit mit umfassender Informationen, muss eine Webtracking-Organisation annehmen, dass einem Nutzer das Webtracking nicht bewusst ist, und deshalb muss sie dann von der Standardeinstellung ausgehen, als ob sie nämlich eine DNT:1 Meldung erhalten hätte, welches den Wunsch des Nutzers anzeigt, dass Tracking unerwünscht ist.

28. Jede für die Zwecke des Webtracking eingesetzte Technologie muss angemessen sein. Weltweit angewandte Datenschutzgrundsätze basieren auf der Vorstellung, dass Daten für spezifizierte, explizite und rechtmäßige Zwecke gesammelt und nicht auf eine Art und Weise weiterverarbeitet werden sollten, die mit solchen Zwecken unvereinbar ist. Die Verarbeitung von Daten sollte angemessen und relevant sein und nicht exzessiv im Verhältnis zu den Zwecken stehen, für die sie gesammelt bzw. weiterverarbeitet werden.

---

[22] Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten (Arbeitspapier WP136), S. 10 URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf .

[23] Die Aufgabenstellung der Tracking Protection Working Group besteht darin, die Privatsphäre und Kontrolle durch die Nutzer zu verbessern, und zwar durch die Definition von Mechanismen zum Ausdruck von Festlegungen durch Nutzer rund um das Webtracking und zum Blocken oder Zulassen von Webtracking-Elementen, http://www.w3.org/2011/tracking-protection/charter .

[24] Im aktuellen Entwurf des DNT-Standards bedeutet das Aussenden von „0“-Meldungen das Einverständnis mit Tracking und „1“ zeigt an, dass Tracking NICHT gewünscht wird.

29. Schließlich muss eine jede Technologie gerichtsfest sein, wenn sie dazu beitragen soll, dem Schutze der Privatsphäre zu dienen. DNT läuft Gefahr, ein Werkzeug zu bleiben, durch das ein Nutzer Wünsche gegenüber Serviceprovidern der Informationsgesellschaft ausdrücken kann, ohne dass dieses ein wirksames Instrument für einen konstruktiven Dialog darstellt. Dies lässt den Nutzer selbst oder eine jede öffentlich-rechtliche (oder private) Körperschaft, die mit die Durchsetzung solcher Wünsche oder Regelungen beauftragt ist (einschließlich der entsprechenden rechtlichen Verpflichtungen, die Auswahl einer Einzelperson zu beachten) im Hinblick auf solche Anbieter mit leeren Händen dastehen. Manche Interessenvertreter der Wirtschaft versuchen die Position zu verteidigen, dass das DNT keine Verpflichtung zur Beachtung eines Wunsches darstellt. Zwar ist diese Interpretation mehr als zweifelhaft, doch bleibt die Tatsache im Raume stehen, dass der Beweis schwer zu führen ist, ob ein solcher Wunsch beachtet oder missachtet wurde.[25] Mit anderen Worten, das DNT könnte aus der Perspektive der Umsetzung ein Placebo anstatt eines wirksamen Heilmittels bleiben, und als solches würde es auch nutzlos bleiben.

Empfehlungen

30. Ungeprüftes Webtracking kann das Gleichgewicht zwischen Dienstanbietern und Privatpersonen auch im Hinblick auf den Schutz der Privatsphäre verändern. Die Arbeitsgruppe unterstreicht, dass Kontext, Transparenz und Kontrolle äußerst wichtige Elemente auch im Kontext des Webtracking bleiben.

31. Um zur Lösung der Gefahren für die Privatsphäre der Privatperson beizutragen, gibt die Arbeitsgruppe die folgenden Empfehlungen an die verschiedenen Interessenvertreter, die im Ökosystem des Webtracking eine Rolle spielen.

Wiedereinführung der Beachtung von Kontext und Zweckbegrenzung als Kerngrundsätze für jede Nutzung personenbezogener Daten:

- Umsetzung von Vorsichtsmaßnahmen für jede (automatisierte) Erhebung, Verarbeitung und die Praxis des Austausches von Daten, sodass in einem bestimmten Kontext gesammelte Daten nicht in einem anderen Kontext angewandt werden können;

- Information über den Zweck der Erhebung von Daten gleich zu Beginn und im Vorhinein und keine Änderung des Zweckes ohne erneute Information und Wahlmöglichkeit.

[25] Ein externes Audit könnte bei der Lösung von zumindest Teilen der oben beschriebenen Probleme eine wichtige Rolle spielen, würde aber andererseits das Ökosystem noch komplexer gestalten.

Wiederherstellung der Transparenz:

- Keine Verwendung unsichtbarer Trackingelemente;

- Mindestens eine verständlich formulierte Mitteilung an den Nutzer, wenn das Anwendungsprogramm im Begriff ist, eine Webtracking-Kennzeichnung an den Empfangsserver zu senden oder eine solche Kennzeichnung vom Ursprungsserver zu empfangen;

- Einblenden einer für den Nutzer ausreichend erkennbaren Anzeige[26] immer dann, wenn Webtracking gerade stattfindet;

- Anzeige eines Hinweises, dass Webtracking gerade stattfindet, der auch für besondere Nutzergruppen, einschließlich der Sehbehinderten, zur Verfügung steht.

Rückverlagerung der Kontrollmöglichkeit zum Nutzer:

- Einrichtung von Mechanismen, die den Nutzern die Ausübung ihres Rechtes auf Privatsphäre und Datenschutz im Internet ermöglichen und kein Einsatz (neuer) Trackingmethoden, welche keine Kontrolle durch den Nutzer ermöglichen; Angebot der Möglichkeit zur expliziten Auswahl bezüglich des Tracking an Nutzer – wenn Browsersoftware installiert, aktiviert oder aktualisiert wird, muss der Nutzer eine Wahlmöglichkeit besitzen;

- Besitzt der Browser keine Anwenderschnittstelle (user interface), sollte die Standardeinstellung so sein, dass das Tracking des Nutzers nicht stattfindet;

- Einräumen der Möglichkeit für Nutzer zur Änderung der Auswahl- und der Änderungseinstellungen nach der ursprünglichen Entscheidung und zu jeder Zeit; Schaffung einer einfachen Prüfmöglichkeit für den Nutzer für die (automatisierten) Wahlmöglichkeiten, die für das Webtracking getroffen wurden; Erinnerung des Nutzers daran, dass Wahlmöglichkeiten bezüglich der (automatisierten) Einstellungen für das Webtracking jederzeit widerrufen werden können und Sicherstellung, dass eine Änderung der Auswahl technisch auf einfache Art und Weise möglich ist, welche der Einzelperson keine ungebührliche Last auferlegt.

- Beachten von Mitteilungen, wenn das Anwendungprogramm meldet, dass Tracking abgelehnt wird;

[26] Ein besonderes Augenmerk muss darauf gerichtet werden, sicherzustellen, dass keine Nutzergruppe des Internets benachteiligt oder anderweitig diskriminiert wird, zum Beispiel aufgrund einer Behinderung.

- Unterlassung des (passiven) Fingerprinting, zum Beispiel durch Mining *[Durchsuchen]* der vom Nutzer generierten Daten (wie zum Beispiel Service Configurations oder User Agent Strings *[Zeichenkette, mit der sich der Browser identifiziert]*), um daraus eine eindeutige Benutzerkennung abzuleiten (Device Fingerprinting), wenn ein Nutzer mitgeteilt hat, dass er Tracking ablehnt.

- Sicherstellen, dass der Einsatz einer jeden Technologie mit dem Ziel, dem Nutzer Wahlmöglichkeiten zu geben, prüffähig ist und von den zuständigen, mit der Umsetzung von Bestimmungen beauftragten privaten oder öffentlich-rechtlichen Körperschaften auch überprüft werden kann, und insbesondere die Umsetzung der in den verschiedenen vorhandenen Rechtssystemen niedergelegten Bestimmungen, welche ihrerseits die Grundlage für den Schutz der Privatsphäre der Privatperson in vielen Rechtsordnungen weltweit bilden.

53rd meeting, 15th and 16th April 2013, Prague, Czech Republic

Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential

Introduction

1. This paper is based on a foundation of respect for the fundamental rights and freedoms of Web users. Although it does not focus on specific technical remedies the paper does assume that the technical action of Web tracking must be lawful, appropriate and that it must operate within a strict framework of those rights. The principles of choice and control – claimed by much of industry – sit at the core of this framework, and those principles must be enacted with precision upon the pillars of clarity, transparency and accountability. The justification for the imposition of Web tracking is not self evident and thus industry and other tracking exponents must continually strive to explore solutions that bring this activity not just squarely within the framework of fundamental rights and privacy, but also in line with the imperative of Privacy by Design.

2. In this working paper, the Working Group addresses the issue of Web Tracking and Privacy. Although no clear definition exists, we will refer to a definition of Web Tracking[1] as the collection, analysis and application of data on user activity from a computer or device while using various services of the Informa-

[1] Cf. van Eijk (2012), The DNA of OBA: unique identifiers, URL: http://www.campusdenhaag.nl/crk/publicaties/robvaneijk.html#definition-of-web-tracking.

tion Society (hereinafter: the Web)[2] in order to combine and analyze it for different purposes, from charitable and philanthropic to commercial. We consider various forms of market research to fall within this definition of Web Tracking, for example outreach measurement (the degree to which users are served with ads across the Web), engagement measurement (the degree to which users interact with services across the Web) and audience measurement (the degree to which micro profiles can be derived from users interacting with services across the Web).[3]

Scope of the Working Paper

3. The paper is addressed to all providers of web sites as well as software developers and service providers offering or using tracking technology. This paper discusses the development of tracking technologies and their possible impact on the privacy of citizens. This paper deals with digital traces left behind when using various services of the Information Society with a Web Browser, including unique identifiers derived from non-cookie based techniques.[4] This includes Web Browsers on other devices, for example smart mobile devicesand smart televisions.

4. This paper does not deal with specific additional risks which may stem from the advent of apps on mobile devices.[5] Nevertheless the principles in this paper should also be applied fortracking mechanisms used in other services.

5. This paper is not about how protective measures can be implemented (e.g., legal requirements for consent). Note that while in some jurisdictions, depending on the purpose of Web Tracking, explicit consent (opt-in) is required, in other jurisdictions, an opt-out for Web Tracking will be considered valid to satisfy the legal framework if certain conditions are met. These include, among other things: adequate notification of processing; transparency in the notification; notification at or before the time of collection; and simple, effective and persistent opt-out methods. A number of restrictions may also be in place, including limiting the

[2] Note that with IP-based technology becoming the backbone of the information society, and integrating many other former „stand alone“ technologies („Convergence“), this may well encompass the use of a telephone (IP telephony), television (IPTV), reading digital newspapers, or any other media consumption using digital tech- nologies (including reading an e-book). For a detailed discussion of the resulting privacy risks cf. theWorking Paper on Privacy Issues in the Distribution of Digital Media Content and Digital Television (Berlin, 4./5.09.2007) of this Group; URL: http://www.datenschutz-berlin.de/attachments/349/digit_en.pdf

[3] JICWEBS Reporting Standards, URL: http://www.abc.org.uk/PageFiles/50/Web Traffic Audit Rules and Guidance Notes version2 March 2013 master.pdf

[4] For example, passive fingerprinting techniques based on hashing the HTTP user agent and/or the IP address of the originating browser.

[5] See, for example, Opinion 02/2013 on apps on smart devices WP 202 issued by the Article 29 Working Party (Art. 29 WP), URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2013/wp202_en.pdf

processing sensitive information such as information on health, information on political or philosophical beliefs and the prevention of the tracking of children.

Background

6. The technical possibilities of monitoring the activities of users on websites have multiplied over the past decade and the emerging „Information Society" has seen several sea changessince then.[6] Web tracking developed from very modest beginnings – when single providers of online services started to monitor their users to find out whether a particular user had been there before and what this user had been doing - into an almost panoptical vision of marketers more recently. In this vision, the marketer seems to be able to monitor every single aspect of the behaviour of an identifiable user across websites. This could potentially become a complete history of the entire Internet usage of a data subject (literally from the cradle to the grave), and could be enriched with profile data from the former „offline world" (including any aspect of our lives data brokers have information about, including financial information as well as information on, for example, leisure, health, political and/ or religious opinions, location information).[7]

7. This development - while greeted and fostered by marketers and other interested parties from the broader business community, and assisted by some policymakers at the national and regional levels – holds an unprecedented risk for the privacy of all citizens in an information society. The worst case scenario is that it would turn the world as we know it into a global panopticon. The offline equivalent would be to have somebody unknown to us constantly looking over our shoulders no matter where we are (in the streets or in the seeming privacy of our homes), or what we do (watching TV, shopping online, reading newspapers, and even more intimate activities), and without knowing when he is looking, and when he isn't.[8]

8. The possible repercussions of such a development are evident and not to be underestimated with respect to their potential gravity. It may annul and do away with some of the core principles of privacy – and notably transparency and control for the individual.[9] To put it more bluntly, this might be the end of the (privacy) world as we know it.

---

[6] The literature review on Web privacy measurement, which has been produced as an outcome of the Conference on Web Privacy Measurement (WPM) gives a more elaborate view on the technologies used for tracking, URL: http://www.law.berkeley.edu/12633.htm

[7] In Customer Relationship Management (CRM) the common terms are Customer Lifetime and Customer Lifetime Value.

[8] To make things even worse, this modernist version of the panopticon would record every single move of any given individual at any given moment in time no matter whether the guard is watching or not.

[9] Tracking as a technology is not transparent. At the technical level, in many cases, the pixels (e.g., web beacons) and mini webpages (e.g., iFrames) are invisible to the human eye

9. The promoters of this vision, on the other hand, claim that these risks either do not exist at all, or that they have tried to address and mitigate these risks at least in part. There is strong resistance from some stakeholders from industry against recognizing that unique identifiers in Web data are personal information. One claim often put forward is that much of the data in use has been de-identified (i.e., anonymised), and that once this has been done, the data is no longer about a person and would therefore not pose a risk to the privacy of citizens. It is also claimed that any behavioural data are linked to machines only and can – this is the claim – in very many instances not be traced back to an individual at all.

10. However, these claims have no scientific proof whatsoever, and ignore the fact that machines – and especially smart phones – are becoming more and more personal devices and allow for an easy link to any given individual user. Traces can also increasingly be linked across different devices. There is also scientific proof that many seemingly anonymous data (e.g., location information of cell phones) can be traced back (i.e., be de-anonymised) to any given user if the database and the timeframe are sufficiently broad. Even worse, more recent academic work suggests that it is impossible in principle to keep „anonymous" data from being de-anonymised if the time slice depicting any given behaviour is sufficiently big (i.e., it is conceptually impossible to guarantee that „anonymous" data cannot be traced back to an individual over time). If this holds true, it is a game changer and will make a couple of core assumptions about how uses of different types of data may or may not affect the privacy ofindividuals useless.[10]

11. In addition, and on a slightly different note, practical daily knowledge also adds to questioning the claims made by industry. While ads may well be addressed to a machine at the technical level, it is not the machine which in the end buys the proverbial beautiful pair of red shoes – it is an individual. Thus, the claim that the processing of behavioural data for marketing is directed „only" at machines in the first place may well be seen as an attempt to blur our vision as societies on the gravity of the problem, when in reality the individual and not the machine is the only instance that can make all such tracking operations a „success" for its proponents (i.e., when the red shoes are finally being bought).

A short history of monitoring technologies

12. In trying to trace back the development described above to its modest beginnings, one milestone we find is the development of „cookie technology" almost 20 years ago. HTTP Cookies were introduced in 1994, first and foremost to solve the „small" problem of reliably implementing a virtual shopping cart. Due to the

[10] Cf. Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, August 2009. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

mostly stateless nature of the Hypertext Transfer Protocol (HTTP), user agents were not able to retain state information until then. Retaining state information was crucial for the virtual shopping cart in order to remember selected items during the shopping experience. Transparency was already then a privacy issue, because the use of cookies was not conveyed to the ordinary user. At the time, cookies were enabled by default in the browser settings and the user was not notified about the use of cookies.[11]

13. To mitigate the privacy and security risk of leaking cookie information to other sites the same origin policy was implemented. This policy meant that cookies could only be read by the same domain that set them. However, it is important to note that recommendations through the World Wide Web Consortium (W3C) propose a new standard, Cross Origin Resource Sharing (CORS)[12] which will permit the sharing of information across specified domains. Although CORS is a voluntary standard, it conflicts with the same origin policy.

14. In 1998, this group[13] addressed various privacy issues connected to the systematic collection or use of personal data on the Web.[14] In its working paper, it addressed P3P (Platform for Privacy Preferences Project), a protocol developed by W3C, which was designed to block third party cookies unless the website the user visited offered a user acceptable P3P policy.[15] However, only one major browser manufacturer implemented the standard. As a result, P3P has not been adopted widely on the Web.

15. Third party cookies have become the lifeblood of the complex digital ad industry. In 2008 marketing executives of Web Tracking companies discussed the future of analytics and site statistics. The future, five years ahead, was envisioned to be an integration of traditional sitevisit statistics (hereinafter: First and Third Party Analytics) and analytics data from other services on the Web including, for example, video, widgets, social networking, gaming and search engines (hereinafter: Web Analytics).[16]

---

[11] RFC 2109, HTTP State Management Mechanism, URL: https://tools.ietf.org/html/rfc2109. Note that current flavors of cookie storage technology include for example flash cookies and the LSOs (Local Shared Objects) used in HTML5 with matching values.

[12] Cross-Origin Resource Sharing, URL: http://www.w3.org/TR/cors/; W3C „Candidate recommendation" status since 29 January 2013 (viewed on 30 May 2013).

[13] International Working Group on Data Protection in Telecommunications

[14] Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the World Wide Web (Hong Kong, 15.04.1998), URL: http://www.datenschutz-berlin.de/attachments/178/priv_en.pdf.

[15] The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Thus users need not read the privacy policies at every site they visit. , URL: http://www.w3.org/P3P/.

[16] Omma Global Measurement 3.0, URL: http://www.webmetricsguru.com/archives/2008/09/measurement-30-on-the-next-5-years-omma-global-day-2/.

16. Today, Web Analytics Data represents a new form of economic value. While this group does not question the benefits that measuring consumer behaviour may bring for (real-time) online behavioural advertising (OBA), it firmly believes that such practice must not be carried out at the expense of individuals‘ rights to privacy and data protection.

Web Tracking

17. Web Tracking involves the collection and subsequent retention, use or sharing of data on individual online behaviour across multiple websites by the use of cookies, JavaScript or any kind of device fingerprinting. Web Tracking technology enables a constant flow of real-time information about users, such as registration data, search activities, behavioural data, site visit statistics and conversion data reflecting how a user responded to individual offers. These data can be used to infer users‘ interests, political opinions or medical conditions. These data can be processed with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual. Data about individual behaviour drives business decisions based on customer profiles. Buying intent may be derived from a person's presumed digital identity. The value of a potential customer is related to the chance to convince him to buy a product.

18. Web Tracking technology is present on mobile devices. A smart mobile device is unlikely to be shared between individuals, therefore making the link between the device and the individual stronger than with, for instance, desktop computers. Mobile devices contain unique device identifiers such as advertising specific identifiers,[17] the Unique Device ID (UDID), Media Access Control (MAC) address, Bluetooth MAC address, Near Field Communications (NFC) MAC address, International Mobile Subscriber Identifier (IMSI, a unique SIM card number) and the International Mobile Equipment Identifier (IMEI). These identifiers cannot be changed by ordinary users. In addition to unique identifiers, smart mobile devices may contain a rich set of data such as user name, password, age, gender, and address book. Smart mobile devices can expose accurate behavioural data on the whereabouts of a user. Precise geolocation data is readily accessible for browsers on smart mobile devices.

19. Web Tracking technology is deployed in various ways. A digital data trail may result from unintentional or unwilling disclosure of data, and may result in unnecessary disclosure of (personal) data. There are multiple ways to generate a digital data trail. For example, a campaign manager for digital ads could assign a unique identifier to the user, browser or device. Another way is to personalize referral

[17] For example, to be able to perform frequency capping (control of the number of times a user has seen an ad), to deliver behavioral ads, and to measure the reach and effectiveness of an advertising campaign.

information by adding audience segment information (micro profiles) while surfing the Web, so other sites participating in the campaign can track the user, browser or device too. A third example is by correlating unique identifiers with data collected from past visits on a specific site. A fourth example is that Web Tracking for a campaign can also take place by combining new tracking data (about a user, browser or device data) with data previously collected on a specific site, or data obtained from another (third) party. A final example involves the use of cookie matching services that connect digital trails from the same user, browser or device with the use of different parts of the Web.[18]

20. Web Tracking consists of several automated steps, starting with the collection of Web data, the retention of these data, and the use of the data. By recombination, correlation and decontextualization, Web data can be used to construct very detailed predictive profiles of individual behaviour. Finally, Web Tracking leads to the actual application of the profile to an individual.[19]

21. Data can be stored in graph databases by various services on the Web.[20] The graph structure enables the emergence of behavioural patterns that would otherwise remain undetected. Web Tracking data in a graph can create meaningful patterns about user behaviour by itself or when combined with other data from various sources. For example, while individual unique identifiers connected directly or indirectly to a user or computer may expose little information about the casual surfer, the collection of unique identifiers reveals a pervasive view of someone‘s habits and browsing behaviour on the Internet. The collection of unique identifiers can be used to construct a digital identity.

Web tracking and the right to privacy and data protection of the individual

22. A key principle across a broad range of international legislative frameworks is the right to privacy that the Internet user has regardless of technology. Key elements are transparency, control and respect for context. The fact that users are unaware that they are being tracked is a privacy risk. Web Tracking as a process utilises a number of technical tools which limit the opportunity for users to be notified. For example, pixels (e.g., web beacons) and mini web pages (e.g., iFrames) are invisible to the human eye and inclusion in a web page will initiate an automatic HTTP request including the opportunity to set and access cookies containing unique identifiers.

[18] See for example URL: https://developers.google.com/ad-exchange/rtb/cookie-guide#what-is.

[19] Cf. also Recommendation CM/Rec(2010)13 of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

[20] A graph is based on graph theory which is a mathematical approach to model pairwise relations between objects. A graph database stores graphs which are essentially structures with nodes, edges, and properties. Theproperties may contain meta information about the nodes and edges:

23. Many web tracking technologies have been developed and deployed in business without providing information to the users whose data is being collected and without giving them any choice. User signals that could be understood as expressing objection to tracking have been disregarded and technical mechanisms against some tracking mechanisms have been actively circumvented, for example, by respawning deleted cookies, (passive) fingerprinting, and circumventing browser settings. Only when these behaviours were detected and were publicly criticized did the interested parties accept their obligation to respect users' free will. In such cases, sometimes opt-out schemes have been added after the fact, often leading to clumsy mechanisms of limited usefulness for the user. These cases have caused great damage to the users' trust in the reliability and honesty of all web service providers and undermine the healthy development of innovative web services.

24. Web Tracking constitutes processing of personal data in many jurisdictions due to the fact that the technology enables the individualization or identification[21] of users and/or making automated decisions about them. An example of such practice might be automatic decisions engines with algorithms in real time bidding platforms for personalized behavioural advertising.

25. There is strong resistance from some interested stakeholders against classifying unique identifiers in Web data as personal information. One claim often put forward is that once data has been de-identified[22] , the data is no longer about a person. It should, however, be clear that a „purpose" element can also be responsible for the fact that information „relates" to a certain person or is about a person.[23]

The potential impact (or lack of impact) of „Do Not Track" (DNT) – a case study

26. In September 2011, the W3C chartered the Tracking Protection Working Group[24]. The group is working on a Do Not Track (DNT) standard. All major browsers have committed themselves to implement the standard (and most have already so implemented the HTTP header), however there remains, amongst those

[21] Recital 26 of the general Data Protection Directive 95/46/EC: Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (...), URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[22] De-identification means deleting, modifing, aggregating, anonymizing or otherwise manipulating data.

[23] Opinion 4/2007 on the concept of personal data (WP136), p. 10 URL: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm.

[24] The mission of the Tracking Protection Working Group is to improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements, URL: http://www.w3.org/2011/tracking-protection/charter.

stakeholders who will honour the DNT:1 request[25], an open discussion on parts of the voluntary standard. Some stakeholders have indicated they will not honour the DNT flag for various reasons. The overall success of DNT is tied to the actual honouring of the DNT flag by receiving organizations and the factual adoption of the DNT standard throughout the Web by all stakeholders.

27. The default settings of DNT and the default actions by the Web Tracking organisation remain crucial once again. For DNT to be an effective instrument to provide user control, it is crucial that those performing Web Tracking can be certain that the DNT signal which they receive is a true indication of the user's wishes. In the absence of fully informed user choice, a Web Tracking organisation must assume that a user is not aware of Web Tracking and therefore assume the default position as if they had received a DNT:1 signal, which indicates a wish from the user not wanting to be tracked.

28. Any technology used for Web Tracking purposes must be proportionate. Data protection principles used worldwide are based on the notion that data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Data processing should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

29. Finally, any technology must be „court-proof" if it is to contribute to serving the protection of privacy. DNT is in danger of remaining a tool through which a user may express wishes to service providers in the information society, without being an effective granular dialogue instrument. This leaves the user himself or any public (or private) body being chartered with enforcing those wishes or rules (and including corresponding legal obligations to honour any such choices made by an individual) empty handed vis-à-vis those providers. Some industry stakeholders try to defend the position that DNT does not constitute an obligation to respect such a wish. While this interpretation is more than doubtful, the fact remains that it is difficult to prove whether such a wish has been respected and or been disregarded.[26] In other words, from an enforcement perspective, DNT could remain a sugar pill instead of being a proper cure and would as such be useless.

Recommendations

30. Unchecked Web Tracking may change the balance between service providers and individuals, including with respect to privacy protection. The Working group

[25] In the current draft DNT standard, sending „0" signals that tracking is fine, while „1" indicates a wish NOT to be tracked.

[26] External audit might play an important role in addressing at least parts of the problems described above, but would on the other hand add even further complexity to the ecosystem.

underlines that context, transparency and control remain crucial elements in the context of Web Tracking.

31. In order to contribute to addressing the risks for the privacy of the individual, the Working Group makes the following recommendations to the different stakeholders who have a part to play in the Web Tracking ecosystem.

Re-introduce respect for context and purpose limitation as core principles for any use of personal data:

- incorporate precautionary principles in any (automated) data collection, processing and sharing practices, so that data collected in one context cannot be applied in another context; and
- inform about the purpose of data collection in advance and do not change the purpose without renewed information and choice.

Bring back transparency:

- Refrain from the use of invisible tracking elements;
- As a minimum, notify the user in an intelligible way when the user agent is about to send/receive a Web Tracking identifier to/from the origin/destination server;
- Display an indicator noticeable enough to the user[27] and whenever Web Tracking is in progress;
- Make an indication that Web Tracking is in progress also available to special groups of users, including the visually impaired.

Put the user back into control:

- implement mechanisms that allow users to exercise their right to privacy and data protection on the Web and do not deploy any (new) tracking mechanisms that do not have a user control mechanism; offer users an explicit choice regarding tracking - when browser software is to be installed, activated or updated, there must be a user choice;

[27] Special consideration must be given to ensure that no group of web users are treated less favourably or are otherwise discriminated against, for example, as a result of a disability.

- if the browser does not provide a user interface, the default setting should be such that the user is not tracked;

- give users the opportunity to reconsider their choice and change settings after the initial decision and at any time; let the user examine the (automated) choices that have been made with regards to Web Tracking in an easy way; and remind the user that choices regarding the (automated) settings for Web Tracking can be revoked at any time and make sure that a revision of any such choices is technically possible in an easy way that does not put any undue burden on the individual;

- honour requests when the user agent is signalling that it does not want to be tracked;

- refrain from (passive) fingerprinting, for example by mining user generated data (such as service configurations, or user agent strings) in order to derive a unique user identifier (device fingerprint) when a user has expressed not wanting to be tracked; and

- ensure that the application of any technology devised to let users make choices is auditable and can be enforced by the competent private or public bodies chartered with enforcing rules, and especially those enshrined in the different existing legal frameworks which provide the foundation of the protection of privacy of the individual in many jurisdictions across the globe.

Arbeitspapier und Empfehlungen zu der Veröffentlichung personenbezogener Daten im Web, der Indexierung des Inhalts von Websites und dem Schutz der Privatsphäre

1. Hintergrund

Einer der wesentlichen Stützpfeiler des Datenschutzes war schon immer das Recht des Betroffenen, über seine Daten zu bestimmen. Ein wesentliches Element dieser Kontrolle ist das Recht, die eigenen Daten gelöscht zu bekommen, wenn sie rechtswidrig verarbeitet werden oder wenn der Betroffene ihrer Verarbeitung nicht länger zustimmt. Der kürzliche Vorschlag der Europäischen Kommission für einen neuen Regulierungsrahmen versucht, dieses Recht zu stärken, indem er ein „Recht auf Vergessen“ durch andere und im Web vorsieht. Dies gilt unbeschadet von solchen Fällen, in denen es ein legitimes und rechtlich gerechtfertigtes Interesse gibt, Daten veröffentlicht und sichtbar zu halten, wie etwa in Medien-

archiven oder zum Zwecke historischer Aufzeichnungen, und es ist klar, dass das Recht auf Vergessen nicht a priori Vorrang vor dem Recht auf freie Meinungsäußerung oder der Medienfreiheit haben kann[1].

Angesichts der Struktur des Webs sind viele Einzelfragen im Hinblick darauf, wie ein solches „Recht auf Vergessen" implementiert werden könnte, sowohl auf der technischen als auch auf der juristischen Seite immer noch ungelöst. Personenbezogene Daten (und jegliche andere Informationen), werden sehr wahrscheinlich öffentlich zugänglich bleiben, wenn sie einmal online veröffentlicht sind. Sogar wenn sie auf der ursprünglichen Webseite gelöscht werden, können sie vor der Löschung auf anderen Seiten verlinkt oder gespiegelt werden. Das Web weiß nicht zu „vergessen" und gegenwärtig ist kein einfaches technisches Werkzeug verfügbar, das die systematische Löschung von Daten im Web sicherstellen könnte (d. h., dem Web das Vergessen beibringen könnte). Kurz gesagt, es gibt keinen „Löschknopf" und es ist zweifelhaft, ob es ihn jemals geben wird.

Dennoch gibt es bereits heute Wege, das Recht des Einzelnen auf Vergessen in einem gewissen Ausmaß zu schützen, indem man sich Werkzeuge zu Nutze macht, die Administratoren von Webseiten zur Verfügung stehen[2], um die freie Verfügbarkeit personenbezogener Daten zu begrenzen, wie auch durch Nutzbarmachung der Möglichkeiten von Suchmaschinen. Im gegenwärtigen Web könnte das Recht auf Vergessen[3] besser als ein „Recht, nicht gefunden zu werden" interpretiert und umgesetzt werden.

2. Die Aussichten der Nutzer, die Kontrolle über ihre personenbezogenen Daten im Web zurückzugewinnen

Die zunehmende Veröffentlichung personenbezogener Daten im Web in den letzten Jahren hat zu neue Herausforderungen und Risiken des Schutzes der Privatsphäre der Bürger Anlass hervorgerufen und gleichzeitig zur Verschärfung existierender Risiken geführt. Das Aufkommen sozialer Netzwerke hat in diesem Zusammenhang eine besonders wichtige Rolle gespielt[4].

---

[1] The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Viviane Reding SPEECH/12/26, Innovation Conference Digital, Life, Design, München, 22. Januar 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26; für eine Kritik dieses Ansatzes s. Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88

[2] Eine solche Sammlung von Werkzeugen sind die Google Webmaster Tools, die es Webmastern ermöglichen, zu sehen, wie Google ihre Site durchsucht und indexiert, und es Webmastern ermöglicht, zu beeinflussen, wie die indexierten URLs angezeigt werden. Ein Link zu den Werkzeugen ist unter http://www.google.ca/webmasters/ verfügbar.

[3] Man beachte, dass der Ausdruck „Recht auf Vergessen" in diesem Papier in einem weiteren Sinne genutzt wird als in dem Entwurf der Datenschutzgrundverordnung der Europäischen Union, und dass dieses Papier keine Aussage enthält, ob ein „Recht auf Vergessen" in dieser Verordnung umgesetzt werden soll oder nicht.

[4] Vgl. Bericht und Empfehlung dieser Gruppe zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum" (Rom (Italien), 3. – 4. März 2008); http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf

Während in diesem Zusammenhang Technologien zur Förderung der Veröffentlichung und verfügbar machen von Daten – einschließlich personenbezogener Daten – im Web dramatische Fortschritte gemacht haben, scheint die Entwicklung von Technologien zur Kontrolle der Verfügbarkeit solcher Daten im Web immer noch in den Kinderschuhen zu stecken. Während Arbeiten für ein „policy-aware Web“[5] in der vergangenen Dekade stattgefunden haben, scheinen wir immer noch weit von jeglichen effektiven, einfach zu nutzenden und breit verfügbaren Werkzeugen entfernt zu sein, die es Bürgern ermöglichen würden, die Kontrolle über ihre eigenen Daten auch nur in einem begrenzten Maß (zurück-) zu gewinnen, wenn diese einmal im Web veröffentlicht worden sind.

Ein mögliches Entwicklungsziel für solche Technologien könnte die Förderung der Löschung aller Kopien von Daten auf jeglichen Geräten oder in jeglichen Speichern sein, in denen sie aufbewahrt werden. Gegenwärtig könnte dies wohl Probleme hinsichtlich der Skalierbarkeit aufwerfen (sogar wenn ein automatisierter Ansatz gewählt wird), besonders, wenn Daten im Laufe der Zeit von der Gemeinschaft der Nutzer im Web verbreitet, weiter verfeinert oder re-kontextualisiert worden sind. Es gibt gegenwärtig keine technische Möglichkeit, alle Kopien eines Objekts und Kopien von Informationen, die mit diesem Objekt im Web zusammenhängen, zu identifizieren und zu lokalisieren. Allerdings könnte dies in einem zukünftigen „policy-aware Web“ möglich sein.

Für neu erzeugte Daten könnte die Verfügbarkeit im Web durch das Setzen von zeitlichen Begrenzungen (Verfallsdaten) im Bezug auf das jeweilige Objekt begrenzt werden. Dies kann auf vielen Wegen erreicht werden. Beispielsweise könnte man Daten mit „aktiver“ (ausführbarer) Software verbinden, die interveniert, wenn das Verfallsdatum erreicht ist, um die Anzeige der Daten auf einem Bildschirm zu deaktivieren oder die Möglichkeit, Screenshots von einem Bild zu erstellen, zu blockieren oder den ursprünglichen Inhalt zu löschen oder zu verschlüsseln. Alternativ können Daten auch mit einem Verfallsdatum „markiert“ werden, sodass alle Server, die mit dem Objekt umgehen, dieses Datum berücksichtigen und die Daten nach dem Verfallsdatum entfernen können.

Weitere interessante Beispiele, wie die Lebenszeit neu generierter Daten im Web angepasst werden kann, werden von einigen anderen neu entstehenden Anwendungen gegeben. Zum Beispiel können Nutzer ein sicheres Overlay-Netz benutzen, das die Sichtbarkeit von Inhalten, wie z. B. einer Nachricht oder eines Bildes durch Nutzung von Ende-zu-Ende-Sicherheit und Zugriffskontrollregeln auf eine Gruppe beschränkt, die zu dem selben Overlay-Netzwerk gehört. In wiederum anderen Anwendungen bleibt eine Textnachricht im Mobilfunk bis zu einem be-

[5] Für einige existierende Vorschläge zur Schaffung eines „policy-aware Web“ vgl. Fußnote 27 auf Seite 10 des „Rome Memorandum“ (Fußnote 4 oben). Das Konzept des policy-aware web kombiniert verschiedene existierende Technologien, namentlich strukturierte Daten, Identitätsmanagement, Zugriffskontrolle und „sticky policies“ (d. h. Nutzungsregeln, die zusammen mit den Daten selbst verbreitet werden).

stimmbaren Verfallsdatum zu einem Nutzer verfügbar. Schließlich können „Nutzer-zentrierte“ Lösungen genannt werden, bei denen der legitime Eigentümer eines Datums selektiv Zugriff darauf gewähren kann, indem er Links zu dem Ort veröffentlicht, wo die Daten in Wirklichkeit nur in einem spezifiziertem Zeitraum gespeichert sind.

Diese Beispiele können als Bausteine für ein zukünftiges „policy-aware Web“ dienen. Allerdings ist eine Menge gründlicher Forschung und Entwicklung nötig, um diese Elemente zu effektiven Werkzeugen für den besseren Schutz der Privatsphäre der Bürger weiterzuentwickeln. Die Arbeitsgruppe ruft die relevanten Akteure in diesem Feld (Industrie, Wissenschaft und Regierungen) dazu auf, ihre Anstrengungen weiter zu verstärken, um hier Fortschritte zu machen.

3. Beschränkung der Verfügbarkeit personenbezogener Daten im Web durch Kontrolle ihrer Indexierbarkeit durch Suchmaschinen

Ein weiter Baustein zur Beschränkung der Verfügbarkeit und ein Beitrag zur Löschbarkeit von Daten im gegenwärtigen Web besteht in der Beschränkung ihrer Verfügbarkeit in den Ergebnissen von Anfragen bei Suchmaschinen[6]. Dies ist bereits jetzt technisch möglich und steht Website-Administratoren als Option zur Verfügung. Sie beruht im Wesentlichen auf zwei Alternativen: Dem „robots.txt-Protokoll“[7] und der Nutzung von an ein Objekt gebundenen Markierungen („tags“), um zu signalisieren, dass ein bestimmter Inhalt oder eine bestimmte Seite nicht von einer Suchmaschine indexiert werden soll.

Das „robots.txt-Protokoll“ arbeitet mit einem kleinen Satz von Instruktionen, die in einer Text-Datei codiert sind (der „robots.txt“-Datei), die im Wurzelverzeichnis einer Domain enthalten ist (z. B. http://example.com/robots.txt). Die Datei wird, falls sie vorhanden ist, von einem Crawler (einem Programm, das von Suchmaschinen genutzt wird, um eine Momentaufnahme einer Website zu erstellen) vor der Indexierung der jeweiligen Website gelesen. Die betreffenden Instruktionen erlauben es, bestimmte Crawler dazu aufzufordern, bestimmte Dateien und/oder Verzeichnisse auf der Website zu ignorieren. Die Instruktionen werden von Crawlern durch Textvergleich alphanumerischer Zeichenketten in der Reihenfolge ausgeführt, in der sie in der robots.txt-Datei enthalten sind. Zu den Anwendungsgrenzen des Protokolls zählen das Fehlen einer ausreichenden Skalierbarkeit,

[6] S. auch Recommendation CM/Rec(2012)3 des Europarats zum Schutz der Menschenrechte in Bezug auf Suchmaschinen.

[7] Das „robots.txt-Protokoll“ wird auch als „Robots Exclusion Protocol“ und als „Robots Exclusion Standard“ bezeichnet. Das Protokoll ist in einem abgelaufenen „Internet Draft“ der IETF definiert, online verfügbar unter http://www.robotstxt.org/norobots-rfc.txt.

dass es mit ftp-Servern nicht funktioniert und dass die Information verloren geht, wenn Inhalte von einer Website kopiert werden[8].

Alternativ können verschiedene Kategorien von Markierungen („tags“) als Attribute einer spezifischen Web-Seite genutzt werden (aber auch in Verbindung mit individuellen Elementen einer spezifischen Seite, wie einem Bild oder einer Datei darin), um zu signalisieren, dass das Objekt/die Seite nicht in die Ergebnisse einer Suchanfrage aufgenommen werden sollte.

Es sollte betont werden, dass diese Ansätze beide vollständig auf Netz-Etikette (d. h. auf die Kooperation der betroffenen Parteien) basieren. Als solche sind sie nur sehr schwer durchzusetzen. Ihre Implementierung durch Websites und Einhaltung durch Suchmaschinen ist völlig freiwillig. Während sie die Risiken der Indexierung, die durch Verlinkung von Webseiten Dritter verursacht werden, abschwächen können, können sie nicht per se sicherstellen, dass ein bestimmtes Informationsobjekt niemals durch eine Suchmaschine indexiert werden wird, besonders, wenn dieses Objekt öffentlich zugänglich ist und von anderen Webseiten mit anderen Zugangsregeln für Crawler verarbeitet werden kann[9].

4. Empfehlungen für Website-Administratoren

Website-Administratoren spielen eine entscheidende Rolle in den beiden oben beschriebenen Kategorien der Löschung, und zwar durch ihre Möglichkeit, die Verfügbarkeit von Daten und die Indexierbarkeit von Objekten zu begrenzen. Um zu den o. g. Zielen beizutragen, gibt die Arbeitsgruppe die folgenden Empfehlungen:

- Betreiber von Websites sollten ihre Nutzer darüber informieren, welche personenbezogenen Daten sie aufbewahren und für welche Zwecke. Sie sollten ihren Nutzern einen einfachen Mechanismus für die Auskunft über ihre personenbezogenen Daten zur Verfügung stellen, und ihnen erlauben, diese zu berichtigen und/oder dauerhaft zu löschen, wie es in der existierenden Datenschutzgesetzgebung vorgesehen ist. Solche Auskunftsmechanismen sollten nutzerfreundlich sein und sollten nicht zu zusätzlichen Kosten für Nutzer führen oder ihnen ungerechtfertigte Verzögerungen oder praktische Belastungen aufbürden.

[8] Manchmal können außerdem Veränderungen bei Web-Inhalten und/oder Präferenzen bei der Indexierung nicht in Suchergebnissen widergespiegelt werden. Es hat sich als bedeutsames Problem erwiesen, Suchmaschinen dazu zu bringen, ihre Indizes zu aktualisieren.

[9] S. in dieser Hinsicht auch die Empfehlungen, die im „gemeinsamen Standpunkt zu Datenschutz bei Suchmaschinen im Internet“, wie 1998 verabschiedet und 2006 überarbeitet, enthalten sind; http://www.datenschutz-berlin.de/attachments/237/WP_Suchmaschinen_de.pdf

- Auf spezifische Anforderung eines Betroffenen, und wenn keine anderen legitimen Interessen oder gesetzlich bindende Beschränkungen existieren, sollten Webmaster die relevante Information umgehend von ihrer Website entfernen. Zusätzlich sollten sie Anbietern von Suchmaschinen signalisieren, den betreffenden Teil der Website zu re-indexieren, um die Daten auch aus dem Suchindex und existierende Kopien im Cache von Suchmaschinen löschen zu lassen.

- Webmaster sollten ihren Nutzern spezifische Werkzeuge zur Verfügung stellen, die es ihnen erlauben, ihre Indexierungs-Präferenzen für die Suche individuell anzupassen[10]. Alternativ könnte auch die Nutzung des „noindex"-meta-tag erwogen werden, dass in dem HTML-Code der betreffenden Seite oder in dem HTTP-Header eingebunden wird oder der sitemap.xml-Datei, um die relevanten Suchpräferenzen im Zusammenhang mit bestimmten Objekten zu signalisieren[11].

- Besondere Sorgfalt sollte beim Schreiben der robots.txt-Datei im Bezug auf die lexikalische und semantische Korrektheit der Anweisungen wie auch ihrer inhärenten logischen Konsistenz gewidmet werden (um gegensätzliche und/oder überlappende Anweisungen zu vermeiden). Es sollte betont werden, dass ein Crawler in Ermangelung *spezifischer Ausschluss-Anweisungen* in der robots.txt-Datei annehmen wird, dass der Administrator die Indexierung der Website oder die Indexierung bestimmter Unterverzeichnisse gestattet (d. h. ein Crawler wird annehmen, dass der Inhalt der Website für Suchmaschinen verfügbar gemacht werden soll).

- Es sollte beachtet werden, dass das robots.txt-Protokoll nicht für die Regelung des Zugriffs auf besonders „riskante" Inhalte wie Verkehrsdaten elektronischer Kommunikationsdienste, Inhalte von SMS-Nachrichten, Speicher von Anrufbeantwortern, Aufenthaltsdaten, Finanzdaten etc. geeignet, noch dass es zur Verhinderung des Zugangs zu spezifischen administrativen Bereichen einer Website gedacht ist. Das robots.txt-Protokoll ist kein Ersatz für Verschlüsselung oder Zugriffskontrollmechanismen.

- Wenn ein Webmaster zu signalisieren beabsichtigt, dass bestimmte Seiten und/oder Dateien nicht von Suchmaschinen indexiert werden sollen, sollte beson-

[10] Vgl. den von der „blogger.com"-Plattform zur Verfügung gestellten Mechanismus, der es Nutzern ermöglicht, ihre Indexierungs-Präferenzen in einem besonderen Formular anzulegen, das bei der Einrichtung des blog-services auszufüllen ist und den Webmaster anweist, wie er seine eigene robots.txt-Datei konfigurieren soll (http://buzz.blogger.com/2012/03/customize-your-search-preferences.html).

[11] Diese Empfehlung ist besonders relevant in dynamischen Umgebungen oder auf komplexen Webseiten, wo die robots.txt-Lösung nicht ausreichend mit der Größe der Webseite skalieren könnte. Ein Beispiel der Nutzung der robots.txt-Kommandos, um einer Suchmaschine das Verfallsdatum einer Seite zu signalisieren, ist verfügbar unter http://googleblog.blogspot.fr/2007/07/robots-exclusion-protocol-now-with-even.html. In gleicher Weise signalisiert die sitemap.xml-Datei, wie oft sich eine Webseite verändern kann, und die Priorität, die ein Webmaster einer URL beimisst, was der Suchmaschine erlaubt, die angemessene Auffrischungsgeschwindigkeit zu wählen. Vgl. auch http://lists.w3.org/Archives/Public/public-privacy/2012OctDec/0224.html

dere Sorgfalt auf die Auswahl der URLs verwendet werden. Tatsächlich könnte, da die robots.txt-Datei öffentlich sichtbar ist, das Vertrauen auf „selbsterklärende" URLs letztlich die Verfügbarkeit der betreffenden Inhalte erhöhen und damit die Vorteile des Protokolls zunichtemachen. Der Inhalt der robots.txt-Datei ist für Hacker besonders wertvoll, wie auch für jede andere Instanz, die versucht, personenbezogene Daten zu verbreiten oder zu beschaffen.

5. Empfehlungen für Suchmaschinen

Als eine ihrer Kernaktivitäten arbeiten Anbieter von Suchmaschinen überwiegend als Informationsvermittler/Intermediäre[12]. Allerdings gibt es auch bestimmte Arten der Verarbeitung, für die sie als eigenständige verantwortliche Stellen agieren.

Insbesondere führen einige Suchmaschinen viele verschiedene Aktivitäten durch, die von der Indexierung von Webseiten bis zur zeitweisen Speicherung des diesbezüglichen Inhalts reichen, um Nutzern das Auffinden der Informationen in Fällen zu ermöglichen, in denen ein Server und/oder Link abgeschaltet/nicht verfügbar ist. Dieses „Caching" stellt eine Wiederveröffentlichung dar, für die der Anbieter der Suchmaschine als verantwortliche Stelle betrachtet wird[13].

Dementsprechend werden die folgenden Empfehlungen für Anbieter von Suchmaschinen unterschieden im Hinblick auf die unterschiedlichen Rollen, die sie spielen.

Bloße Indexierung

- Suchmaschinen sollten die von den Websites in Bezug auf die Inhalte, die sie enthalten ausgedrückten Präferenzen immer respektieren, sei es durch die robots.txt-Datei oder durch andere „noindex"-Markierungsmechanismen, einschließlich Anweisungen zu Verfallsdaten. Solche Indexierungs-Präferenzen können vor der ersten Durchsuchung der Website ausgedrückt werden, oder nachdem sie schon durchsucht worden ist. Im letzteren Fall sollten Aktualisierungen der von einer Suchmaschine durchgeführten Indexierung so schnell wie möglich durchgeführt werden.

[12] Vgl. die Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen (WP 148) der Artikel-29-Datenschutzgruppe der Europäischen Datenschutzbeauftragten (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf). Man beachte, dass diese Angelegenheit gegenwärtig vor dem Europäischen Gerichtshof verhandelt wird.

[13] Wie in der Stellungnahme zu Suchmaschinen von der Artikel-29-Datenschutzgruppe der europäischen Datenschutzbeauftragten (WP 148) betont wird, ist „… jegliche Zwischenspeicherung von auf indexierten Webseiten enthaltenen, personenbezogenen Daten über diesen aus Gründen der technischen Verfügbarkeit notwendigen Zeitraum hinaus (…) als eine unabhängige Neuveröffentlichung anzusehen. Nach Auffassung der [Artikel-29-] Arbeitsgruppe liegt die Verantwortung für die Einhaltung der Datenschutzgesetze hier beim Anbieter derartiger Caching-Funktionalitäten in seiner Rolle als Verantwortlicher für die Verarbeitung der personenbezogenen Daten, die in den zwischengespeicherten Veröffentlichungen enthalten sind."

- Suchmaschinen sollten die Effizienz ihrer Kommunikationskanäle mit Webmastern erweitern, um schnell über jegliche Veränderung der Indexierungs-Präferenzen in Kenntnis gesetzt zu werden, die von Webmastern durch die geeigneten Anweisungen des robots.txt-Protokolls ausgedrückt werden, oder von jeder Veränderung von Objekten innerhalb einer Website. Die Aktualisierungs/Berichtigungs-Prozeduren sollten so datenschutzfreundlich wie möglich sein – insbesondere sollten keine zusätzlichen personenbezogenen Daten von Nutzern verlangt werden, die verlangen, dass bestimmte personenbezogene Daten aktualisiert/berichtigt werden.

- Suchmaschinen sollten ihre Crawling-Häufigkeit den Suchpräferenzen der Webmaster anpassen. Sie sollten auch jegliche Anforderungen von Webmastern zur Re-Indexierung ihrer Webseiten oder von Teilen davon infolge der Löschung oder Berichtigung von personenbezogenen Daten unverzüglich ausführen.

- Da es bisher keine konsistente Interpretation der in einer robots.txt-Datei oder anderen Signalisierungsmechanismen für Indexierungspräferenzen (z. B. Metatags, sitemap.xml.-Dateien) enthaltenen Anweisungen durch Suchmaschinen gibt, ist schwer vorherzusagen, welchen Einfluss solche Mechanismen auf die Indexierung einer Website durch die verschiedenen Crawler haben wird. Es ist wünschenswert, dass sich Suchmaschinen in dieser Hinsicht auf einen „modus operandi" einigen. Die für die einzelnen Befehle anwendbaren Mechanismen sollten in klarer Weise auf einer Seite beschrieben werden, auf die von Nutzern leicht zugegriffen werden kann (z. B. von den Hauptseiten des Suchmaschinenportals).

- Suchmaschinen sollten in einem größeren Maße in die Unterstützung von Website-Administratoren eingebunden sein, indem sie Anleitungen und/oder Werkzeuge für die automatisierte Analyse von Indexierungs-Präferenzen zur Verfügung stellen. Dies wird Administratoren ermöglichen, zu überprüfen, welche Effekte die von Ihnen gegebenen Befehle in Bezug auf die Indexierung haben werden.

- Suchmaschinen sollten die Terminierung und Kriterien des „crawling", das sie auf einer bestimmten Website durchführen, klarer spezifizieren, so dass Administratoren und Nutzer in vernünftiger Weise abschätzen können, wie lange eine bestimmte Information als Suchergebnis verfügbar bleibt.

Zeitweise Speicherung von durchsuchten Informationen

- Suchmaschinen sollten spezifische Crawler implementieren, wenn sie beabsichtigen, Daten nach verschiedenen Kategorien und für verschiedene Zwecke

(z. B. generelle Indexierung, Nachrichten, Bilder, etc.) zu gruppieren, um Administratoren von Webseiten zu ermöglichen, den Kontext, in dem Informationen veröffentlicht werden, besser zu kontrollieren.

- Bei der Indexierung einer Website sollten Suchmaschinen komplexere und granularere Instruktionen für ihre Crawler zulassen, wie beispielsweise die folgenden:

  – Die Erlaubnis zur Indexierung von Informationen für bestimmte Zwecke (z. B. Allzweck-Suchmaschinen vs. Nachrichten-Suchmaschinen, etc.)[14];

  – die Erlaubnis, Informationen zeitweise für bestimmte Zwecke zu speichern, einschließlich diesbezüglicher Zeitbegrenzungen (z. B. caching, snippets);

  – die Erlaubnis, Informationen für bestimmte Zwecke an Dritte weiterzugeben;

  – die Erlaubnis, die abgefragten Informationen für bestimmte Anwendungsfälle[15] basierend auf dem Vorkommen von Eigenschaften, wie geografischer Lage oder IP-Adressräumen zu verarbeiten.

- Wo die Durchsuchung eine zeitweisen Speicherung von Inhalten einer Website für andere Zwecke zur Folge hat, als es Nutzern zu ermöglichen, auf diese Inhalte im Falle zuzugreifen, dass der betreffende Server/das betreffende Netzwerk abgeschaltet/nicht verfügbar ist, sollten Suchmaschinen die Administratoren von Websites mit eindeutigen, spezifischen Informationen über den Zeitablauf versorgen und über technische Mechanismen, die für diese Speicherung gelten.

- Suchmaschinen sollten aufgrund spezifischer Anforderungen von Webmastern durch deren Such-Präferenzen jegliche Cache-Kopie der von Webseiten abgerufenen Daten unverzüglich löschen, und sollten von der weiteren Verarbeitung dieser Daten absehen, um das Risiko der Verbreitung der Daten und deren übermäßiger Exponierung zu begrenzen.

---

[14] Vgl. z. B. die von der italienischen Kartellbehörde verlauteten Feststellungen infolge einer Beschwerde der italienischen Vereinigung der Zeitungsverleger gegen Google. Danach verpflichtete sich Google öffentlich auf eine Reihe von Maßnahmen, um Verlage mit Werkzeugen auszustatten, die ihnen dabei helfen sollen, zwischen der Indexierung von Inhalten auf der allgemeinen Suchmaschine und der Indexierung auf der Nachrichten-Suchmaschine zu unterscheiden.

[15] Wegen der zunehmend komplexen Anwendungsfälle, die auf die von Suchmaschinen durchsuchten Informationen anwendbar sind, könnte es angemessen sein, das gegenwärtige Muster umzudrehen, nachdem Crawler eine Information lesen dürfen, wenn eine Anweisung formal inkorrekt ist oder von dem Crawler nicht interpretiert werden kann. Wenn es sich als unmöglich erweist, eine komplexe Menge von Anweisungen zu interpretieren, sollte dies automatisch als ein Verbot der Indexierung/Speicherung durch den Crawler interpretiert werden.

6. Ein abschließender Vorbehalt

In diesem Papier hat die Arbeitsgruppe Werkzeuge für die Kontrolle der Verfügbarkeit (personenbezogener) Daten im Web untersucht, die heute für Nutzer, Webmaster und Suchmaschinen verfügbar sind, zumeist gegründet auf die Begrenzung der Verfügbarkeit von Inhalten auf einer Website entweder durch Anwendung von (automatisierten) Löschmechanismen[16] oder durch die Implementierung von Protokollen zur Signalisierung von Suchpräferenzen. Es sollte daran erinnert werden, dass letztere immer noch auf einfachen ein/aus- (binären) Regeln für Crawler beruhen, die vor über 15 Jahren entworfen wurden. Im Gegenzug sind Suchmaschinen über die Jahre immer komplexer geworden und der ehe simple Inklusions-/Exklusionsmechanismus, der dem betreffenden Protokoll zugrunde liegt, ist nicht länger vollständig fähig, das fortwährend wachsenden Ausmaß der Gewinnung und Speicherung von Daten zu bewältigen. Es sollte z. B. herausgestellt werden, dass die Verfügbarkeit von Daten (einschließlich Daten, die Nutzer über sich selbst preisgeben), in Kombination mit Gesichtserkennungstechniken und Aufenthaltsinformationen, letztendlich eher die Indexierung von Individuen als nur von Inhalten oder Informationen ermöglichen kann. Ein vordringliches Augenmerk auf diese Aspekte ist deswegen notwendig.

Ein anderer, zukünftiger technologischer Durchbruch für den besseren Schutz personenbezogener Daten im Web könnte die Entwicklung des „policy-aware, semantic Web" sein, in dem Daten untrennbar mit Attributen (z. B. einer „Bedeutung") und Zugriffsregeln verknüpft werden könnten. Dies würde auf der einen Seite die Schaffung von neuen Beziehungen zwischen Daten ermöglichen und das Konzept einer vernetzten Welt erweitern, und auf der anderen Seite effektivere Mechanismen zur Erkennung und Auffindung von Inhalten ermöglichen, und potenziell auch von Kopien von Informationen, die mit diesem Objekt in Beziehung stehen, gestützt auf den Abgleich von Attributen (anstatt auf einfache Textvergleiche, wie dies heute stattfindet). Dies macht es vorstellbar, Informationen von einer Vielzahl von Websites zu entfernen und Suchergebnisse von Websites zu entkoppeln, und damit jegliche unbeabsichtigte Verbreitung von Daten zu vermeiden[17].

Natürlich sollte die Benutzbarkeit des Web nicht unterminiert werden und es muss eine Balance zwischen Innovation und den Grundrechten des Individuums auf Datenschutz und Schutz der Privatsphäre gefunden werden. Die Möglichkeit der

[16] Es ist hervorzuheben, dass aufgrund der öffentlichen Natur des Web andere Zugriffskontrollmechanismen wie die Authentifizierung von Nutzern und/oder Verschlüsselung von Daten implementiert werden sollten, wenn der Administrator einer Website Inhalte aus der „Öffentlichkeit" entfernen möchte.

[17] Google hat kürzlich eine Aktualisierung seines Suchalgorithmus angekündigt, die die Platzierung von Sites mit einer großen Anzahl von Mitteilungen über Löschungen herunterstufen wird und die nur in Fällen der Verletzung von Urheberrechten angewandt werden soll (http://insidesearch.blogspot.fr/2012/08/an-update-to-our-search-algorithms.html oder http://www.google.com/insidesearch/howsearchworks/).

Einführung granularerer Mechanismen, die nicht auf der einfachen Exklusions-/Inklusionsregel basieren, sollte weiter bedacht werden, aber eher darauf gerichtet sein, Betroffene in die Lage zu versetzen, ihre eigenen Suchpräferenzen besser auszudrücken und die Information mit dem angemessenen Kontext zu verbinden (z. B., indem es Betroffenen ermöglicht wird, zu signalisieren, ob eine bestimmte Information noch aktuell oder relevant ist, oder das Vorkommen jeglicher Ereignisse, die Auswirkungen auf diese Informationen gehabt haben könnten). Dies würde den Betroffenen mehr Möglichkeiten eröffnen als die einfache Wahl zwischen pauschaler, überschießender Verfügbarkeit im Web oder einem kompletten Verzicht auf neue Technologien.

Es gibt bedeutende und wachsende ökonomische Interessen sowohl bei Suchmaschinen als auch bei Administratoren von Websites, die auf die größtmögliche Verfügbarkeit von Daten durch die Implementierung der Indexierung von Daten und Informationen dringen. Diese Indexierung von Websites dient den ökonomischen Interessen bestimmter Marktteilnehmer und die Entfernung öffentlich zugänglicher Webinhalte oder die Signalisierung, dass solche Inhalte nicht durch eine Suchmaschine indexiert und abgerufen werden sollten, wird zwangsläufig Auswirkungen auf Geschäftsmodelle und die Marktdynamik haben. Eine Zusammenarbeit der verschiedenen Interessenvertreter ist notwendig, um die diesbezüglichen Interessen mit der Notwendigkeit des Schutzes der Privatsphäre angemessen in Einklang zu bringen.

Working Paper and Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy

1. Background

One of the main pillars of data protection has always been the data subjects' right to control their own data. An essential element of this control is the right to have one's data deleted if they are processed illegally or if the data subject no longer consents to their processing. The recent proposal by the European Commission for a new regulatory framework tries to strengthen this right by providing for a "right to be forgotten" by others, and on the Web. This is without prejudice to those cases where there is a legitimate and legally justified interest to keep data published and visible, such as in media archives or for the purposes of historical

records, and it is clear that the right to be forgotten cannot take precedence *a priori* over freedom of expression or freedom of the media [1].

In view of the present structure of the Web, many issues with respect to how such a "right to be forgotten" could be implemented are still unsolved on the technical as well as on the legal side. Personal data (and any other information), once published online, will very likely remain publicly available. Even if they are deleted on the original website, they may have been linked to or mirrored on other sites before deletion. The Web does not know "how to forget" and there is no simple technical tool available at present which could ensure the systematic deletion of data on the Web (i.e., which could teach the Web how to forget). In short, there is no "erase button" and it is doubtful whether there will ever be one.

However, there are ways to protect the individual's right to be forgotten to a certain extent even today by leveraging tools available to website administrators[2] to limit the exposure of personal information on the Web as well as by making use of/harnessing the power of search engines. On the current Web, the right to be forgotten[3] might better be interpreted and implemented as a "right not to be found".

2. The prospects of regaining control of the exposure of personal data on the Web

The increasing publication of personal data on the Web over the past year has given rise to new challenges and risks for the privacy of citizens, while aggravating existing risks at the same time. The advent of social networks has played a particularly crucial role in this context[4].

While technologies fostering the publication and making available of data – including personal data – on the Web have made dramatic progress in this context, the development of technologies to control the availability of such data on the Web still seems to be in its infancy. While work on a "policy-aware web"[5] has taken

[1] The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Viviane Reding SPEECH/12/26, Innovation Conference Digital, Life, Design Munich, 22 January 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26; for a critique of this approach see Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88

[2] One such set of tools are the Google Webmaster Tools, which allow webmasters to see how Google crawls and indexes their site and allows webmasters to influence how the URLs that are indexed are displayed. A link to the tools is available at http://www.google.ca/webmasters/.

[3] Note that the term „right to be forgotten" is used in a broader sense in this paper than in the proposed EU Privacy Regulation, and that this paper does not make any statement on whether a "right to be forgotten" can be implemented in that regulation or not.

[4] Cf. the Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" of this Group – (Rome (Italy), 3./4.03.2008); http://www.datenschutz-berlin.de/attachments/897/675.36.5.pdf

[5] For some existing proposals for creating a "policy-aware Web" cf. footnote 27 on page 10 of the „Rome Memorandum" (footnote 4 above). The concept of the policy-aware Web combines several existing technologies, namely structured data, identity management, access control, and sticky policies (i.e., use policies that travel with the data itself).

place over the past decade, we still seem to be far from any effective, easy-to-use and widely available tools which would enable citizens to (re-) gain even a limited amount of control over their data once they have been published on the Web.

One possible design goal for such technologies could be fostering the deletion of all copies of that data from any device or storage area where it is retained. At present, this may well pose problems of scalability (even with an automated approach), especially if specific data has been disseminated on the Web or further elaborated or re-contextualized over time by the community of Web users. There is currently no technical way to identify and locate all copies of an item and copies of information correlated with that item on the Web. However, this may be possible in a future "policy-aware Web".

For newly generated data, exposure on the web could be limited by setting time limits (expiration dates) on the given item. This can be accomplished in many ways. For instance, one might equip data with "active" (executable) software which intervenes when the expiration deadline is reached in order to disable data display on a screen, or disable the ability to make screenshots of the image, or ultimately to delete or encrypt the original content. Alternatively, data can be "tagged" with an expiration date, so that all servers handling that item can take account of that date and remove the data after the expiry date.

Further interesting examples of how to customize the lifetime of newly generated data on the Web are given by some other emerging applications. For instance, users may utilise a secure overlay network restricting visibility of content, such as a post or image, to a community belonging to the same overlay network by using end-to-end security and access control policies. In yet other applications, a mobile text message remains available to a user until a configurable expiration date. Finally, reference can be made to "user centric" solutions, where the legitimate owner of a data may selectively provide access to it, releasing links to the place where the data is actually stored only within a specified timeframe.

These examples may serve as building blocks for a future "policy-aware Web". However, a lot of thorough research and development is necessary to further develop these elements to be effective tools for better protecting the privacy of citizens. The Working Group calls upon the relevant actors in this field (Industry, academia, and governments) to further strengthen their efforts to make progress in this field.

3. Restricting availability of personal data on the Web by controlling their indexability by search engines

Another building block for restricting availability and contributing to erasability of data on the current Web is to restrict its availability in the results of queries to

search engines[6]. This is already technically feasible and available as an option to website administrators. It essentially relies on two alternatives: the robots.txt protocol[7], and the use of "tags" attached to an item to signal that a specific con-tent or web page should not be indexed by a search engine.

The robots.txt protocol works by way of a small set of simple instructions coded in a text file (the robots.txt file) placed in the root directory of a domain (e.g., http://example.com/robots.txt). This file is read, if present, by a crawler (software program used by search engines to give a "snapshot" of a website) prior to indexing the relevant website. The instructions in question allow requesting *specific crawlers* to ignore *specific files and/or directories* in the website. The instructions are executed by crawlers after text matching of alphanumerical strings according to the sequence followed by the instructions in the robots.txt file. Limitations of the protocol include a lack of sufficient scalability, it does not work with ftp-servers and the information is lost when content is copied from a website[8].

Alternatively, different categories of "tags" can be used as attributes of a specific web page (but also in connection with individual elements of a specific page, such as an image or a file therein) to signal that the item/page should not be included in the results of a search query.

It should be emphasized that these approaches are both entirely based on net etiquette (i.e., on the co-operation of the parties involved). As such, they are very difficult to enforce. Their implementation by websites, and adherence to by search engines, is strictly voluntary. Thus, while they can mitigate the risk of indexing determined by linkage from third party sites, they cannot ensure per se that a given item of information will never be indexed by a search engine, in particular if that item is publicly accessible and can be processed by other websites with different crawler access rules.[9]

4. Recommendations to Website Administrators

Website administrators play a crucial role in both categories of erasability described above, namely through their capabilities for limiting the exposure of data

[6] See also Recommendation CM/Rec(2012)3 of the Council of Europe on the protection of human rights with regard to search engines.

[7] The robots.txt protocol is also referred to as the Robots Exclusion Protocol and the Robots Exclusion Standard. The protocol is defined in an expired IETF Internet Draft, available online at http://www.robotstxt.org/norobots-rfc.txt.

[8] Changes in web content and/or indexing preferences can sometimes not be reflected in search results as well. Getting search engines to update their indexes when sites change has proven to be a significant problem.

[9] In this regard, see also the Recommendations contained in the IWGDPT's "Common Position on Privacy Protection and Search Engines" as adopted in 1998 and revised in 2006; http://www.datenschutz-berlin.de/attachments/238/search_engines_en.pdf.

and restricting the indexability of items. In order to contribute to the goals set out above, the Working Group makes the following recommendations:

- Website operators should inform their users about what personal data they retain and for what purposes. They should provide their users with an easy mechanism to access their personal data, and allow them to correct and/or to delete them permanently, as provided for by existing privacy legislation. Such access mechanisms should be user friendly and should not result in any additional cost to users or impose unjustified delays or operational burdens.

- Upon a data subject's specific request, and if no other legitimate interests or legally binding constraints exist, webmasters should promptly remove the relevant piece of information from their website. In addition, they should signal to search engine providers to re-index the respective part of the website, in order to have the data also deleted from the search index and any cache copies of the search engines.

- Webmasters should provide their users with specific tools to allow customizing their search indexing preferences[10]. Alternatively, consideration could be given to using the "noindex" meta-tag – to be included in the HTML code of the relevant page or in the HTTP header – or the sitemap.xml file to signal the relevant search preferences in connection with specific items[11].

- Special care should be taken in writing the robots.txt file as regards the lexical and semantic correctness of the instructions as well as their inherent logical consistency (to prevent conflicting and/or overlapping instructions). It should be pointed out that *failing specific exclusion instructions* in the robots.txt file, a crawler will assume that the administrator allows site indexing or the indexing of specific sub-directories (i.e., a crawler will assume that website contents should be made available to search engines).

- It should be observed that the robots.txt protocol does not lend itself to regulating access to especially "risky" contents such as traffic data generated by electronic communications services, SMS-message contents, voice mail storage, location data, financial data etc., nor is it aimed at preventing access to specific

[10] Cf. the mechanism provided by the "blogger.com" platform enabling users to set up their indexing preferences in a specific form to be filled when subscribing to the blog service, instructing the webmaster on how to configure his own robots.txt file (http://buzz.blogger.com/2012/03/customize-your-search-preferences.html).

[11] This recommendation is especially relevant in dynamic environments or complex websites, where the robots.txt solution might not scale enough with the size of the website. An example of the use of the robots.txt commands to signal a search engine the expiration date of a page may be found at http://googleblog.blogspot.fr/2007/07/robots-exclusion-protocol-now-with-even.html. Similarly, the sitemap.XML file signals how frequently a web page may change, and the priority level that the webmaster attributes to a URL, allowing the search engine to potentially select the appropriate refresh rate. Cf. also http://lists.w3.org/Archives/Public/public-privacy/2012OctDec/0224.html.

administrative areas in a website.[12] The robots.txt protocol does not replace cryptography or access control mechanisms.

- If a webmaster intends to signal that specific pages and/or files should not be indexed by search engines, special care should be dedicated to the selection of URLs. Indeed, since the robots.txt file is publicly visible, relying on "self-explanatory" URLs might ultimately enhance exposure of the relevant contents and thereby void the benefits of the protocol. The contents of the robots.txt file are especially valuable to hackers as well as to any entity seeking to disseminate/acquire personal data.

5. Recommendations to Search Engines

As one of their core activities, search engine providers work mainly as information brokers/intermediaries[13]. However, there are also certain types of processing in respect of which they act as separate data controllers.

In particular, some search engines perform many different activities, ranging from indexing of websites, to storing the respective contents temporarily to enable users' retrieval of information in case a server and/or link is down/unavailable. This caching constitutes a re-publication for which the provider of the search engine is deemed to be a data controller[14].

Accordingly, the following recommendations for search engine providers are distinguished according to the different roles played by them.

Mere Indexing

- Search engines should always respect indexing preferences expressed by websites with respect to the content they host, whether via the robots.txt file or via other "noindex" tagging mechanisms, including expiration date commands. Such indexing preferences can be expressed before the first crawling of the

[12] In July 2011, about 8000 SMS messages received on the mobile network of MegaFon were indexed by Yandex, a Russian search engine, making content data and addressees' mobile phone numbers publicly available. Similarly, 43,000 SSNs belonging to Yale University students were disclosed in August 2011 after being indexed by Google because they had been stored in a public subdirectory of an ftp server.

[13] Cf. the Opinion on data protection issues related to search engines (WP148) by the Article 29 Working Party of European Privacy Commissioners (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf). Note that this issue is currently before the European Court of Justice.

[14] As pointed out in the Opinion on search engines by the Article 29 Working Party of European Privacy Commissioners (WP148), "… any caching period of personal data contained in indexed websites beyond (…) technical availability, should be considered an independent republication. The [Article 29] Working Party holds the provider of such caching functionalities responsible for compliance with data protection laws, in their role as controllers of the personal data contained in the cached publications."

website or once it has already been crawled. In the latter case, updates on the indexing performed by a search engine should be carried out as soon as possible.

- Search engines should enhance the effectiveness of their communication channels with webmasters in order to be notified rapidly of any change in the indexing preferences, expressed by webmasters by means of the appropriate commands of the robots.txt protocol, or any modification of items within a website. The update/rectification procedures should be as privacy-friendly as possible – in particular, no additional personal data should be required from users that request certain items of personal information to be updated/rectified.

- Search engines should adjust their crawling rate according to the search preferences expressed by webmasters. They should also execute any requests by webmasters for reindexing their websites or parts thereof following the deletion or correction of personal data without undue delay.

- Since there is as yet no consistent interpretation by search engines of the instructions written in a robots.txt file or in other indexing preferences signaling mechanisms (e.g., metatags, sitemap.xml files), it is difficult to foresee what impact such mechanisms will have on indexing of a website by the different crawlers. It is desirable that search engines agree on a "modus operandi" in this regard. The mechanisms applying to the individual instructions should be described clearly on a page that should be easily accessible by users (e.g. from the main pages of the search engine portals).

- Search engines should be involved to a greater extent in supporting website administrators by providing tutorials and/or tools for the automated analysis of indexing preferences. This will enable administrators to check what effects the instructions they are giving will produce in terms of indexing.

- Search engines should more clearly specify timing and criteria of the "crawling" they perform on a given website, so that administrators and users can reasonably gauge how long a given piece of information will remain available as a search result.

Temporary Storage of Crawled Information

- Search engines should implement specific crawlers if they intend to group data according to different categories and for different purposes (e.g., general indexing, news, images, etc.) in order to allow website administrators to better control the context in which information will be published.

- When indexing a website, search engines should accept more complex and more granular instructions for their crawlers such as the following:

  – Permissions to index information for specific purposes (e.g., general-purpose search engines vs. news search engines, etc.)[15];

  – Permissions to temporarily store information for specific purposes, including the respective time limits (e.g. caching, snippets);

  – Permissions to communicate information to third parties for specific purposes;

  – Permissions to process the retrieved data for specific use-cases[16] based on the occurrence of features such as geographic area or IP address ranges.

- Where crawling is followed by temporary storage of site contents for purposes other than that of enabling users to access those contents in the event the given server/network is down/unavailable, search engines should provide site administrators with clear-cut, specific information on the timeline and technical mechanisms applying to said storage.

- Search engines, upon specific requests issued by webmasters through their search preferences, should promptly delete any cached copy of the data retrieved from websites, and should abstain from further processing these data, mitigating in this way the risk of data dissemination and overexposure.

6. Final Caveat

In this paper, the Working Group has explored tools for controlling the availability of (personal) data on the Web which are available today to users, webmasters and search engines, mostly based on limiting contents exposure on a website either through the application of (automatic) deletion mechanisms[17] or via the implementation of search preference signaling protocols. It should be recalled that the latter still rely on simple on/off (binary) rules applying to crawlers, and were

[15] Cf. e.g. the findings reported by the Italian Antitrust Authority following a complaint lodged by the Italian Federation of News Publishers against Google. Thereafter Google committed itself publicly to complying with a set of undertakings so as to provide publishers with tools that should help them distinguish between indexing of contents on the generalist search engine and indexing on the news search engine.

[16] Given the increasingly complex use-cases that apply to the information crawled by search engines, it might be appropriate to consider reversing the current pattern, whereby crawlers are allowed to read information if an instruction is formally incorrect or cannot be interpreted by the crawler. If it proves impossible to interpret a complex set of instructions, the latter should be interpreted by default as a ban on indexing/storage by the crawler.

[17] It is worth highlighting that, due to the public nature of the Web, when a website administrator wants to remove content from the "public sphere", other access control mechanisms should be implemented such as user authentication and/or data encryption.

designed over 15 years ago. Conversely, search engines have become increasingly sophisticated over the years and the rather simple inclusion/exclusion mechanism underlying the protocol in question is no longer fully capable to cope with the ever increasing scope of data retrieval and storage. It should, for instance, be emphasized that the availability of data (including data which users disclose about themselves), in combination with facial recognition techniques and location data, can ultimately allow the indexing of individuals rather than simply of contents, or of information. An urgent focus on these aspects is therefore necessary.

Another prospective technological breakthrough for better protecting personal data on the Web may be the advent of the "policy-aware, semantic Web", where data could be inextricably linked with attributes (e.g., a "meaning") and access rules. This would allow, on the one hand, for the creation of new relations between data and enhance the concept of an interconnected world whilst providing, on the other hand, more effective mechanisms to identify and locate content, and potentially also copies of information correlated with that item based on attribute matching (rather than by simple text matching as it happens today). This would make it conceivable to remove information from a multiplicity of websites and to de-link search results from websites, thus avoiding any unintended data dissemination[18].

Of course, usability of the Web should not be undermined and a balance must be struck between innovation and individuals' fundamental rights to privacy and data protection. Further consideration should be given to the option of introducing more granular mechanisms that are not based on the simple exclusion/inclusion rule, but rather attempt to enable data subjects to better express their own search preferences and link the information to the appropriate context (for instance, by allowing data subjects to signal whether or not a given piece of information is still current or relevant, or the occurrence of any events that may have impacted on that information). This would afford data subjects wider options than the simple choice between blanket overexposure on the Web or a complete abstention from new technologies.

There are major, growing interests of an economic nature vested in both search engines and website administrators pushing for the widest possible availability of data through the implementation of data and information indexing. This indexing of web sites serves the economic interest of certain market players, and removing publicly available web contents or signaling that such contents should not be indexed and retrieved via a search engine is bound to impact on market dynamics and business models. Co-operation of the various stakeholders is necessary to appropriately reconcile the interests in question with the need for privacy protection.

[18] Google recently announced an update to its search algorithm which will lower the ranking of sites with high numbers of removal notices, to be applied only in cases of copyright infringements (http://insidesearch.blogspot.fr/2012/08/an-update-to-our-search-algorithms.html or http://www.google.com/insidesearch/howsearchworks/).

54. Sitzung, 2. und 3. September 2013, Berlin

Arbeitspapier zum Recht auf vertrauliche Telekommunikation

Angesichts der jüngsten Berichte über die Aktivitäten von Nachrichtendiensten erinnert die Arbeitsgruppe daran, dass sie bei verschiedenen Gelegenheiten die Bedeutung des Telekommunikationsgeheimnisses als Menschenrecht hervorgehoben hat[1]. Telekommunikation findet heutzutage meist grenzüberschreitend statt, so dass die Unterscheidung zwischen nationaler und internationaler Telekommunikation überholt ist. Telekommunikation und insbesondere das Internet sind lebensnotwendige Technologien für Einzelne und Gesellschaften im 21. Jahrhundert. Beide hängen von der berechtigten Erwartung der Nutzer ab, dass die Kommunikation *im Grundsatz* frei von Überwachungs- und Abhörmaßnahmen bleibt. Dies betrifft sowohl Inhalts- als auch Verbindungs- oder Nutzungsdaten und andere digitale Spuren. Wenn diese Vertraulichkeit als Grundregel bedroht ist, dann ist die Grundstruktur freier Gesellschaften in Gefahr. Die Kommunikationsüberwachung durch staatliche Behörden im Allgemeinen[2] und Nachrichtendienste im Besonderen, kann für legitime Zwecke notwendig sein, sie muss aber die *Ausnahme* bleiben und darf nicht zur Regel werden. Um den Grundsätzen der Offenheit, Transparenz und Rechenschaftspflicht zu genügen, sollten Vorkehrungen getroffen werden, um der Öffentlichkeit die Sicherheit zurückzugeben, dass Abhörbefugnisse rechtsmäßig, angemessen und verhältnismäßig genutzt werden.

Die Arbeitsgruppe fordert die Regierungen deshalb dazu auf:

1. das Telekommunikationsgeheimnis als wesentlichen Teil des weltweit garantierten Menschenrechts auf Schutz der Privatsphäre anzuerkennen[3];

---

[1] Gemeinsame Erklärung zur Kryptografie (12.9.1979) – http://www.datenschutz-berlin.de/attachements/172/crypt_de.pdf; gemeinsamer Standpunkt im Hinblick auf das Abhören privater Kommunikation, 23. Sitzung, 15.4.1998, Hongkong – http://www.datenschutz-berlin.de/attachements/904/inter_de.pdf; gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilateraler Abkommen zum Datenschutz („10 Gebote zum Schutz der Privatheit im Internet"), 28. Sitzung, 14.9.2000 Berlin – http://www.datenschutz-berlin.de/attachements/216/tc_de.pdf; Arbeitspapier zur Überwachung der Telekommunikation, 21. Sitzung, 27.3.2002 Auckland – http://www.datenschutz-berlin.de/attachements/912/wptel_de.pdf; die Charta von Granada zum Datenschutz in einer digitalen Welt, 27. Sitzung, 15.–16.4.2010, Granada – http://www.datenschutz-berlin.de/attachements/793/kopie_von675.41.21.pdf?1307526860. Der Europäische Gerichtshof für Menschenrechte hat in seiner Rechtsprechung Art. 8 der Europäischen Menschenrechtskonvention entsprechend interpretiert, vgl. Fall Weber und Seravia ./. Deutschland, Entscheidung vom 29. Juni 2006, mit weiteren Nachweisen.

[2] Zur unterschiedlichen Rechtslage weltweit vgl. International Data and Privacy Law, Vol. 2 No. 4 (2012), Special Issue on Systematic Government Access to Private Sector Data.

[3] Das Recht auf Vertraulichkeit der privaten Korrespondenz ist besonders erwähnt in Art. 12 der UN-Menschenrechtserklärung, Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte und Art. 8 der Europäischen Menschenrechtskonventionen.

2. das Telekommunikationsgeheimnis als Menschenrecht in einem völkerrechtlichen Vertrag zu stärken. Einschränkungen sollten auf das begrenzt werden, was in einer demokratischen Gesellschaft unbedingt notwendig ist;

3. sich auf internationale Regeln zu verständigen, mit denen der Zugriff staatlicher Stellen auf Daten bei Internetanbietern und der Einsatz von nachrichtendienstlichen Mitteln im Internet begrenzt wird;

4. für größere Transparenz und öffentliche Rechenschaftspflicht von Regierungsstellen bezüglich der Ergebnisse rechtmäßiger Überwachungsmaßnahmen zu sorgen[4]; dies schließt transparente Regeln zur Klassifizierung und Deklassifizierung ein[5];

5. sicherzustellen, dass jeder betroffene Mensch unabhängig von seiner Nationalität das Recht auf nachträgliche Benachrichtigung, auf Löschung oder Korrektur seiner Daten und auf Zugang zu den Gerichten hat;

6. den Bürgerinnen und Bürgern zu gestatten, dass sie frei Werkzeuge zur sicheren Kommunikation erforschen, schaffen, verteilen und nutzen, und sie dazu zu ermutigen; kein Bürger und keine Bürgerin sollte allein deshalb überwacht werden, weil er oder sie solche Werkzeuge nutzt;

7. eine effektive und unabhängige Kontrolle von Überwachungstätigkeiten sicherzustellen, die von der Polizei, Nachrichtendiensten oder in ihrem Auftrag von privaten Datenverarbeitern[6] durchgeführt werden.

54th meeting, 2nd and 3rd September 2013, Berlin

Working Paper on the Human Right to Telecommunications Secrecy

In view of recent reports on the activities by intelligence services the Working Group recalls that it has on several occasions stressed the importance of telecom-

[4] Der Europäische Gerichtshof für Menschenrechte hat im Fall Youth Initiative for Human Rights ./. Serbien, Urteil vom 25. Juni 2013, klargestellt, dass Nachrichtdienste der Informationsfreiheitsgesetzgebung unterliegen.

[5] Vgl. die Grundsätze 11–17 der weltweiten Prinzipien zur nationalen Sicherheit und zum Informationsrecht von Tshwane vom 12. Juni 2013.

[6] Vgl. Grundsatz 6 der weltweiten Prinzipien von Tshwane.

munications secrecy as a human right[1]. Most telecommunications today is taking place across borders therefore the distinction between national and international telecommunications has become obsolete.Telecommunications and in particular the Internet are essential technologies for individuals and societies in the 21st century. Both depend on the legitimate expectation of users that communications in principle are free from surveil- lance and interception. This applies to contents as well as metadata and other digital traces. If this confidentiality by default is threatened the very fabric of free societies is at risk. Interception of communications by government agencies in general[2] and intelligence services in particular can be necessary for legitimate reasons but it must be the exception, not the rule. To comply with principles of openness, transparency and accountability, there should be mechanisms to re-assure the public that interception powers are being used lawfully, appropriately and proportionally.

The Working Group therefore urges governments:

1. To recognize telecommunications secrecy as an essential part of the globally acknowledged human right to privacy;[3]
2. To strengthen telecommunications secrecy as a human right in an international convention. Restrictions should be limited to what is strictly necessary in a democratic society;
3. To agree on international rules limiting government access to data stored by Internet service providers and signals intelligence on the Internet;
4. To provide for greater transparency and public accountability of government agencies as to the results of lawful interceptions[4]; this includes transparent rules on classification and declassification[5];

---

[1] Common Statement on Cryptography (12.09.1997) – http://www.datenschutz-berlin.de/attachments/172/crypt_en.pdf ; Common Position on Public Accountability in relation to Interception of Private Communications, 23rd meeting, 15 April 1998, Hong Kong – http://www.datenschutz-berlin.de/attachments/904/inter_en.pdf; Ten Commandments to protect Privacy in the Internet World – Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements, 28th meeting, 14 September 2000, Berlin – http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf ; Working Paper on Telecommunications Surveillance, 31st meeting, 27 March 2002, Auckland – http://www.datenschutz-berlin.de/attachments/912/wptel_en.pdf; The Granada Charter of Privacy in a Digital World, 47th meeting, 15./16 April 2010, Granada – http://www.datenschutz-berlin.de/attachments/794/675.40.11_Endfassung.pdf. The European Court of Human Rights in its jurisprudence has interpreted Art. 8 of the European Human Rights Convention along similar lines, see Case of Weber and Saravia v. Germany, Decision of 29 June 2006, with further references.

[2] For the diverse legal situation globally cf. International Data Privacy Law, Vol. 2 No.4 (2012), Special issue on Systematic Government Access to Private Sector Data.

[3] The right to private correspondence is specifically mentioned in Article 12 of the UN Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR).

[4] The European Court of Human Rights in the case of Youth Initiative for Human Rights v. Serbia, Judgment of 25 June 2013 has clarified that intelligence agencies are within the scope of freedom of information legislation.

[5] See Principles 11–17 of the Tshwane Global Principles on National Security and the Right to Information of 12 June 2013.

5. To ensure that every data subject regardless of nationality has the right to be notified ex post, to have his data deleted and corrected and of access to justice;

6. To allow and encourage citizens to freely research, create, distribute and use tools for secure communications; no citizen should be monitored simply on the ground that he or she is using such tools;

7. To ensure effective and independent oversight with regard to surveillance activities carried out by police and intelligence agencies or on their behalf by private processors[6].

Arbeitspapier zum Datenschutz bei Überwachung aus der Luft

Hintergrund

Überwachung ist das Beobachten von Verhalten, Aktivitäten oder anderen sich verändernden Informationen, um etwas oder jemanden zu beeinflussen, zu verwalten, zu steuern oder zu schützen. Sie beinhaltet häufig die Beobachtung von Individuen oder Gruppen durch Regierungsstellen, obwohl es einige Ausnahmen gibt, wie z. B. die Überwachung der Verbreitung von Krankheiten, bei der die Verbreitung einer Erkrankung in einer Gemeinschaft beobachtet wird, ohne Individuen direkt zu beobachten oder zu kontrollieren.

Überwachung aus der Luft ist das Erheben von Informationen, normalerweise von Bildern oder Videoaufnahmen, von einem Luftfahrzeug aus. Seit die Internationale Konferenz der Datenschutzbeauftragten zum ersten Mal über Luftüberwachung durch Satelliten diskutierte[1], hat es weitreichende technologische Entwicklungen gegeben. Während Satelliten-basierte Dienste wie Google Earth gegenwärtig keine besonderen Risiken für die Privatsphäre des Einzelnen bilden, solange nur Einzelbilder mit begrenzter Auflösung gesammelt werden, verhält es sich mit tief fliegenden Überwachungsplattformen wie Drohen anders. Während

[6] See Principle 6 of the Tshwane Global Principles.

[1] S. Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Fernmeldegeheimnisses und der Satellitenkommunikation und gemeinsame Erklärung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, 29. Oktober 1992, Sydney, in: Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983 – 2006, S. 42; http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

die Nutzung von Drohnen für militärische (Gefechts-) Zwecke Gegenstand einer – aufgrund von Geheimhaltung – begrenzten öffentlichen Debatte ist, wurde eine vergleichbare Diskussion über die zivile Nutzung dieser Technologie zum Zwecke der Sammlung von Informationen und deren Konsequenzen bisher vernachlässigt. Die Geschichte der Satellitentechnologie seit 1989 zeigt jedoch, dass Aufklärungstechnologien, die früher auf eine militärische Nutzung beschränkt waren, auch für die zivile Nutzung verfügbar werden können.

Überwachungsplattformen können für eine Vielzahl von Zwecken genutzt werden, einschließlich:

a) Fernerkundung: Die Nutzung verschiedener Sensoren (visueller, Infrarot- oder Nahinfrarot-Spektrum, Gamma-Strahlen, biologischer und chemischer), um die Gegenwart von Chemikalien, Mikroorganismen und anderen biologischen Faktoren, radioaktive Materialien, Waffen usw. zu erkennen;

b) Kommerzielle Luftüberwachung: Viehbeobachtungen, Flächenbrandkontrolle, Pipeline-Sicherheit, Gebäudesicherheit, Präzisionsackerbau, Verkehrswacht und Anti-Piraterie[2];

c) Erkundungen von Bodenschätzen: Durchführung geophysikalischer Untersuchungen zur Vorhersage der Lage von Öl-, Gas- und Mineralvorkommen, Überwachung von Öl- und Gaspipelines und vergleichbarer Infrastruktur, Vergleich der tatsächlichen Größe von Ackergrundstücken, für die Subventionen gezahlt wurden, mit Angaben in den dazugehörigen Antragsformularen[3];

d) Wissenschaftliche Forschung: Wetterbeobachtung einschließlich der Nahbeobachtung gefährlicher Wettersysteme wie Wirbelstürmen oder Nutzung in schwierigen Klimabedingungen wie in der Antarktis;

e) Suche und Rettung: Suche nach vermissten Personen, Schadensabschätzung nach Natur- (oder durch Menschen verursachte) Katastrophen; und

f) Naturschutz: Beobachtung der Bewegung von Tieren, Erkennung und Überwachung der Verbreitung von Unfällen mit Gefahrenstoffen, Waldbranderkennung, Fischereischutz, etc.

---

[2] Die US-Unternehmen Skybox Imaging und Planet Labs planen die Nutzung von Flotten leichter Mikrosatelliten zur Erdüberwachung in Echtzeit. Sie ermöglichen privaten Investoren den Kauf und das Herunterladen von Bildmaterial, vgl. http://www.nytimes.com/2013/08/11/business/microsatellites-what-big-eyes-they-have.html?_r=0 (abgerufen am 20. Oktober 2013).

[3] Vgl. das europäische „Integrated Administration and Control System (IACS) http://ec.europa.eu/agriculture/direct-support/iacs/index_en.htm , das auf die Verhinderung von Betrug bei Landwirtschaftssubventionen gerichtet ist. IACS beinhaltet Satellitenüberwachung.

Überwachungsplattformen

Eine Vielzahl von Plattformen[4] oder Fahrzeugen wird zur Luftüberwachung verwendet oder kann dazu verwendet werden, einschließlich:

a) Starrflügler: ein Starrflügelflugzeug ist ein Flugzeug, das mithilfe von Flügeln fliegt, die Auftrieb erzeugen, der durch die Vorwärtsbewegung des Fahrzeugs und die Form der Flügel ermöglicht wird. Die Flügel eines Starrflügelflugzeugs sind nicht notwendigerweise steif; Drachen, Hängegleiter und Flugzeuge, die „wing-warping" oder variable Geometrie benutzen, werden alle als Starrflügelflugzeuge angesehen;

b) Drehflügler: Der Begriff Drehflügel beschreibt eine Tragfläche, die um eine annähernd vertikale Achse rotiert, wie die eines Helikopters oder Tragschraubers beim Fliegen;

c) Unbemannte Flugsysteme (Unmanned Aircraft Systems – UAS). Ein unbemanntes Fluggerät (Unmanned Aircraft – UA), landläufig als Drohne bezeichnet, ist ein Fluggerät ohne einen menschlichen Piloten an Bord. Sein Flug wird entweder autonom von Computern innerhalb des Fahrzeugs kontrolliert oder über Fernbedienung durch einen Piloten am Boden oder in einem anderen Fahrzeug. UAS können Starr- oder Drehflügler sein und einzeln oder in Schwärmen (die untereinander und mit der zentralen Kontrollinstanz am Boden kommunizieren) betrieben werden, oder

d) Sonstige: Ein Aerostat ist ein Fahrzeug, das primär durch die Nutzung von dem Auftrieb von Gasen in der Luft bleibt, die leichter sind als Luft, und die einem Fahrzeug mit fast derselben Dichte wie Luft Auftrieb gewähren. Aerostaten beinhalten Frei- und/oder Fessel-Ballons, Zeppeline oder andere steuerbare Luftschiffe, die angetrieben oder antriebslos sein können.

Jede dieser Plattformen hat verschiedene Betriebseigenschaften wie Betriebshöhe, Geschwindigkeit, Reichweite, Höchstflugdauer (d. h. wie lange kann die Plattform in der Luft bleiben), die Fähigkeit zu schweben, und Nutzlast-Kapazität.

Überwachungstechnologien

Verschiedene Überwachungstechnologien können von den o. g. Plattformen getragen werden; die genaue Traglast hängt von einer Reihe von Faktoren wie Aufgabe, Wetterbedingungen, Nutzlast-Kapazität, die Reichweite des Sensors, sein

[4] Eine andere Kategorisierung findet sich auf Seite 2 bei Stanley, J. und Crump, C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report datiert Dezember 2011 (online verfügbar unter http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

Sichtfeld und seine Auflösung, usw. Sensoren umfassen (sind aber nicht notwendigerweise beschränkt auf):

a) Sichtbares Spektrum: Diese Sensoren haben typischerweise die Form von Kameras, einschließlich hochauflösenden und full-motion-Videosystemen[5]; sie erlauben fortlaufende Überwachung in Echtzeit und die Speicherung des gesamten Videomaterials;

b) Infrarot (IR): Diese Art von Sensoren erkennt Energie, die vom Ziel ausgesendet oder reflektiert wird. Die meisten IR-Sensoren sind passiv, obwohl sie in Verbindung mit einer IR-Beleuchtungsquelle benutzt werden können. Sie können durch Rauch, Nebel, Dunst und andere atmosphärische Verschleierungen besser „sehen" als Kameras für sichtbares Licht;

c) Nachtsicht: Die Fähigkeit bei schlechten Lichtbedingungen zu sehen, gestützt auf eine Kombination von ausreichendem Spektralbereich (d. h. wieviel vom elektromagnetischen (EM) Spektrum das Gerät erkennen kann) und ausreichendem Helligkeitsbereich (d. h. wieviel Licht ist notwendig, um ein brauchbares Bild zu erzeugen). Nachtsichttechnologien können grob in drei Hauptkategorien eingeteilt werden:

   1. Bildverstärkung: Diese Technologien arbeiten nach dem Prinzip der Vergrößerung der Menge empfangener Photonen aus verschiedenen natürlichen Quellen sowie Sternenlicht oder Mondlicht. Beispiele für solche Technologien umfassen Nachtgläser und Restlicht-Kameras;

   2. Aktive Ausleuchtung: Diese Technologien funktionieren nach dem Prinzip der Kopplung von Bildverstärkungstechnologien mit einer aktiven Lichtquelle im Nahinfrarot (NIR) oder Kurzwellen-Infrarot (shortwave infrared – SWIR)-Band. Ein Beispiel solcher Technologien sind Restlicht-Kameras; und

   3. Wärmebild-Aufklärung: Diese Technologien funktionieren durch Erkennung der Temperatur-Differenz zwischen den Hintergrund- und den Vordergrund-Objekten.

d) Radar: Radar nutzt Funkwellen des Hochfrequenz-Spektrums, um die Entfernung, Höhe, Richtung oder Geschwindigkeit eines Objekts zu bestimmen.

[5] Die U.S. Army erwarb kürzlich eine 1.8 Gigapixel-Kamera zur Nutzung in ihren Drohnen. Diese Kamera (Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System – ARGUS IS) bietet 900 mal so viele Pixel wie eine 2-Megapixel-Kamera eines Mobiltelefons; sie wurde zu niedrigen Kosten unter Nutzung von 368 Kamera-Mikrochips aus Mobiltelefonen gebaut. Sie kann Objekte am Boden in 65 Meilen Entfernung aus einer Höhe von 20.000 Fuß verfolgen. Vgl. *US Army unveils 1.8 gigapixel camera helicopter drone*, BBC NEWS (29. Dezember 2011), http://www.bbc.com/news/technology-16358851. Ein aufschlussreiches Video ist verfügbar unter: http://www.youtube.com/watch?v=QGxNyaXfJsA, abgerufen am 2. April 2013.

Radar kann auch dazu genutzt werden, Objekte am Boden wie z. B. Fahrzeuge zu identifizieren und zu verfolgen (beispielsweise unter Nutzung von luftgestütztem Schrägsichtradar (Side Looking Airborne Radar – SLAR)); und

e) Spezialsensoren: Eine Reihe von Spezialsensoren (z. B. zur Erkennung von Spuren chemischer, biologischer, nuklearer, radiologischer und explosiver Materialien; Nummernschild-Scanner; akustische Sensoren, etc.) können ebenfalls von luftgestützten Überwachungsplattformen getragen werden.

Kombinationen dieser Sensortypen können Organisationen die Möglichkeit zur Durchführung von Luftüberwachung unter beinahe jeglichen Bedingungen bieten.

Auswirkungen auf die Privatsphäre

Es gibt eine Reihe von Aspekten der Überwachung, die Datenschutzbedenken hervorruft, einschließlich der Tatsache, dass Überwachung unsichtbar, intrusiv, willkürlich und kontinuierlich ist.[6] Obwohl diese Aspekte im Zusammenhang mit elektronischer Kommunikation beschrieben wurden, sind sie auch auf die Luftüberwachung anwendbar:

a) Unsichtbar: Abhängig von der Größe, der Einsatzhöhe, der Fähigkeiten der Sensoren usw., kann es unmöglich sein, Luftüberwachung (entweder die Plattform selbst oder die genutzten Sensoren) zu entdecken. Die von der Überwachung Betroffenen müssten auf deren Aufdeckung durch die Organisation selbst bauen, die die Überwachung durchführt oder auf die Aufdeckung durch einen Dritten. Die von unsichtbarer Überwachung Betroffenen haben weniger Möglichkeiten, die Organisation zur Verantwortung zu ziehen, die die Überwachung durchführt;

b) Intrusiv: Der Bandbreite möglicher Operationsbedingungen für Plattformen zur Luftüberwachung und die Fähigkeiten ihrer Sensoren verstärken die Intrusivität von Luftüberwachung (sie können fast alles und jedes „sehen“);

c) Willkürlich: Luftüberwachung deckt im allgemeinen ein Gebiet ab, das Individuen und Aktivitäten einschließt, die eine Überwachung nicht erfordern, was in der überschießenden Sammlung von Informationen resultiert; und

[6] Freiwald, Susan: „A First Principles Approach to Communications Privacy“, veröffentlicht in Stanford Technology Law Review (2007 STAN. TECH. L. REV. 3), datiert 2007. Abrufbar unter http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf .

d) Kontinuierlich: Aufkommende Plattformen zur Luftüberwachung kombinieren zunehmende Betriebsdauer und die Fähigkeit, auf ein Gebiet zu „starren", um eine wirksame, fortdauernde Überwachung eines beliebigen Gebiets zu erzeugen[7].

Diese Charakteristiken geben Anlass zu einigen spezifische Befürchtungen hinsichtlich des Schutzes der Privatsphäre[8]:

a) Schleichende Ausweitung des Einsatzes („Mission Creep"): Obwohl die meisten Menschen die Nutzung von Luftüberwachung (z. B. für die Entdeckung und Überwachung von Naturkatastrophen) oder zur Nutzung unter spezifischen, begrenzten Umständen bei der Strafverfolgung wahrscheinlich unterstützen würden, scheint es unvermeidlich, dass zukünftig weitere Privatsphäre-invasive Nutzungen für solche Technologien gefunden werden;

b) Verfolgung: Die Fähigkeit, die Überwachung einer erweiterten Fläche über erweiterte Zeiträume aufrechtzuerhalten, birgt die Möglichkeit, dass Individuen und Fahrzeuge fortlaufend verfolgt werden können;

c) Proliferation, weil die Kosten für UAS-Technologien rapide fallen. UAS können von Privatpersonen zur Nutzung als „persönliche" oder „Do it yourself"-UAS gekauft oder gebaut werden.

Intrusiver für die Privatsphäre als Videoüberwachung

Die Auswirkungen von Videoüberwachung auf die Privatsphäre sind seit Jahren Gegenstand von Debatten gewesen, und viele Datenschutzbehörden haben Richtlinien zu den notwendigen Sicherungsmaßnahmen bei deren Nutzung herausgegeben. Wie oben erläutert verfügen Luftüberwachungssysteme aus verschiedenen Gründen über ein größeres Potenzial zur Verletzung der Privatsphäre als Videoüberwachungssysteme, einschließlich:

- Luftüberwachungssysteme können viel mehr verschiedene Sensoren nutzen als Videoüberwachungssysteme.

[7] Die U.S. Air Force hat die Gorgonenblick- („Gorgon Stare") Technologie entwickelt, eine kugelförmige Anordnung von neun Kameras, die in eine Drohne eingebaut und fähig ist, Bewegtbilder ganzer Städte aufzunehmen („With Air Force's Gorgon Drone 'we can see everything'", http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html)

[8] Eine Erörterung der verschiedenen potentiellen Datenschutzbedenken findet sich auf Seite 11 bei Stanley, J. und Crump, C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", ACLU Report datiert Dezember 2011 (abrufbar unter http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

- Die Installation von Videoüberwachung erfordert normalerweise den Zugang zu und die Kontrolle über die entsprechenden Grundstücke; diese ist für Luftüberwachungssysteme nicht erforderlich, insbesondere für Orte im Freien.

- Abhängig von der Flughöhe und anderen Faktoren (z. B. Miniaturisierung) können Luftüberwachungssysteme von den überwachten Personen schwieriger – wenn nicht unmöglich – zu entdecken sein als die meisten Videoüberwachungssysteme.

- Luftüberwachungssysteme können ohne jegliche Verzögerung angewandt werden; sie benötigen keine Installation oder Konfigurationen vor Ort.

Dies deutet in klarer Weise darauf hin, dass die Sicherungsmaßnahmen für Videoüberwachungseinrichtungen, obwohl sie einen Minimalstandard anzeigen, im Zusammenhang mit Luftüberwachungssystemen nicht als ausreichend angesehen werden können und durch spezifische, den verschiedenen Luftüberwachungssystemen und Nutzungsszenarien angemessene Maßnahmen angepasst und ergänzt werden müssen.

Daher sollten bestimmte neue, essentielle Sicherungsmaßnahmen auf nationaler Ebene von den Gesetzgebern unter Berücksichtigung möglicher Unterschiede zwischen dem öffentlichen und dem privaten Sektor verabschiedet werden. Darüber hinaus werden internationale Vereinbarungen notwendig sein, um die Herausbildung eines „globalen Panoptikums“ zu verhindern, da Luftüberwachung nicht an Landesgrenzen Halt macht.

Empfehlungen

Die zunehmende Nutzung von Luftüberwachung wird wahrscheinlich Bedenken darüber verstärken, wie die individuelle und kollektive Privatsphäre im täglichen Leben geschützt werden kann, egal ob sie von Strafverfolgungsbehörden oder anderen Einrichtungen der öffentlichen Verwaltung, oder von Privatunternehmen, oder von Bürgern zu Freizeitzwecken betrieben wird. Wenn Luftüberwachung ein zunehmend normaler Bestandteil der heutigen Gesellschaft wird, und die Gesellschaft deren Gegenwart als normal akzeptiert, ist es vorstellbar, dass die Erwartungen der Gesellschaft an den Schutz der Privatsphäre in der Öffentlichkeit ernstlich untergraben werden könnten. Es ist wichtig, eine angemessene Balance zwischen den Bedürfnissen der Strafverfolgung, der öffentlichen Sicherheit etc. auf der einen Seite und den legitimen Interessen der Individuen am Schutz der Privatsphäre auf der anderen Seite sicherzustellen. In diesem Sinne gibt die Arbeitsgruppe die folgenden Empfehlungen:

a) Die Nutzung von Luftüberwachung sollte auf spezifische Zwecke[9] beschränkt werden (z. B. die Suche nach vermissten Personen, die Überwachung von Grenzen, legitime private Zwecke, wie den Zugang zu Informationen durch Journalisten);

b) Die Nutzung personenbezogener Daten, wie beispielsweise Bildern, die durch Behörden aus der Luft gesammelt werden, sollten unter Richtervorbehalt stehen;

c) Die Öffentlichkeit sollte über die Nutzung von Luftüberwachung im größtmöglichen Ausmaß unterrichtet werden; dies erfordert z. B., dass jedes UAS mit der Fähigkeit, Informationen über eine Datenverbindung zu übertragen, seine GPS-Positionsdaten, Fähigkeiten und Angaben zum Eigentümer (z. B. die Behörde, das Unternehmen oder die Privatperson, die für die jeweilige Plattform oder das jeweilige Fahrzeug verantwortlich ist), in Echtzeit an eine geeignete Behörde übermittelt wird und dass diese Behörde die Aufenthaltsinformationen als „Open Data" in Echtzeit verfügbar macht;

d) Die Überwachung sollte auf eine Fläche beschränkt werden, die so klein wie möglich ist (durch Begrenzung der Sichtfelder des Sensors), um die Wahrscheinlichkeit für eine „überschießende Erhebung" zu minimieren;

e) Es sollten stringente Kontrollen darüber eingeführt werden, wie Luftüberwachungsinformationen genutzt werden können und wer auf diese Informationen Zugriff hat. Für Notfälle (z. B. die Suche nach vermissten Personen) können Ausnahmen gemacht werden; und

f) Es sollte immer eine menschliche Kontrollinstanz eingebunden sein, so dass, falls es Probleme oder ungewöhnliche Umstände gibt (z. B., dass das UAS in ein Wohngebiet abdriftet), diese so schnell wie möglich angegangen werden können.

Die Arbeitsgruppe wird die Entwicklungen in diesem Bereich im Lichte der sich rasant entwickelnden Technologie weiterhin genau beobachten.

---

[9] Die American Civil Liberties Union (ACLU) beschreibt die folgenden Auflagen für die Nutzung von Drohnen:
a) **Nutzungsbeschränkungen:** Drohnen sollten von Strafverfolgungsbehörden nur unter Richtervorbehalt oder in Notfällen angewendet werden, oder wenn es spezifische und benennbare Gründe zu der Annahme gibt, dass die Drohne Beweismittel in Bezug auf eine bestimmte Straftat sammeln wird;
b) **Datenspeicherung:** Bilder sollten nur aufbewahrt werden, wenn der berechtigte Verdacht besteht, dass sie Beweismittel für ein Verbrechen enthalten oder für eine laufende Untersuchung oder ein laufendes Gerichtsverfahren relevant sind;
c) **Richtlinien:** Nutzungsrichtlinien für innerstaatliche Drohnen sollten durch die Repräsentanten der Öffentlichkeit festgelegt werden und nicht durch Polizeibehörden; die Richtlinien sollten klar, schriftlich und der Öffentlichkeit zugänglich sein; und
d) **Missbrauchsverhinderung & Verantwortlichkeit:** Die Nutzung innerstaatlicher Drohnen sollte Gegenstand offener Überprüfungen und angemessener Aufsicht zur Verhinderung von Missbrauch sein.
Siehe http://www.aclu.org/blog/tag/domestic-drones; siehe auch die bei EPIC aufgeführten Quellen unter http://www.epic.org/privacy/drones , in der verschiedene Gesetzentwürfe erwähnt werden, die diese Themen betreffen und gegenwärtig im U.S.-Kongress behandelt werden.

Working Paper on Privacy and Aerial Surveillance

Background

Surveillance is the monitoring of behavior, activities, or other changing information, for the purpose of influencing, managing, directing, or protecting someone or something. It often involves observation of individuals or groups by government organizations, although there are some exceptions, such as disease surveillance, which monitors the progress of a disease in a community without directly observing or monitoring individuals.

Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle. Since the International Conference of Data Protection and Privacy Commissioners first discussed issues of aerial surveillance by satellites in 1992[1], there have been far-reaching technological developments. Whereas satellite-based services such as Google Earth at present do not pose particular risks to individual privacy as long as only snapshots with limited resolution of imagery are collected, the situation is different with regard to low flying surveillance platforms such as drones. Whereas the use of drones for military (combat) purposes is the subject of some limited – due to classification – public debate, similar debate about civilian uses of this technology for information collection purposes and their consequences has so far been neglected. The history of satellite technology since 1989 shows however that reconnaissance technology formerly restricted to military use can eventually become available for civilian use as well.

Surveillance platforms can be used for a wide range of purposes, including:

a) Remote sensing: the use of a variety of sensors (visual, infrared or near infrared spectrum, gamma ray, biological and chemical) to detect the presence of chemicals, microorganisms and other biological factors, radioactive materials, weapons and so on;

b) Commercial aerial surveillance: livestock monitoring, wildfire mapping, pipeline security, home security, precision farming, road patrol and anti-piracy[2];

[1] Cf. Report of the Working Group on Data Protection in Telecommunications on problems relating to the secrecy of telecommunications and satellite communications and Common Statement of the 14th International Conference of Data Protection and Privacy Commissioners, 29 October 1992, Sydney, in: International Documents on Data Protection in Telecommunications and Media 1983 – 2006, p. 51; http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

[2] The US-companies Skybox Imaging and Planet Labs are planning to deploy fleets of lightweight microsatellites to engage in Live Earth Screening. They are allowing private investors to buy and downlink imagery, cf. http://www.nytimes.com/2013/08/11/business/microsatellites-what-big-eyes-they-have.html?_r=0 (seen on 20 October 2013).

c) Resource exploration: perform geophysical surveys in order to predict the location of oil, gas and mineral deposits, monitoring the integrity of oil and gas pipelines and related infrastructure, comparing the real size of farmland for which subsidies have been received with claims in the corresponding application forms[3];

d) Scientific research: weather observations, including close monitoring of dangerous weather systems such as hurricanes, or use in severe climates such as the Antarctic;

e) Search and rescue: searching for missing persons, damage assessment following a natural (or man-made) disaster; and

f) Conservation: monitoring movements of animals, detecting and monitoring hazardous material spills, forest fire detection, fishery protection, etc.

Surveillance Platforms

A variety of platforms[4], or vehicles, has been or can be used for aerial surveillance, including:

a) Fixed Wing: a fixed-wing aircraft is an aircraft capable of flight using wings that generate lift caused by the vehicle‘s forward airspeed and the shape of the wings. The wings of a fixed-wing aircraft are not necessarily rigid; kites, hang-gliders and aeroplanes using wing-warping or variable geometry are all regarded as fixed-wing aircraft;

b) Rotary Wing: the term rotary wing describes an airfoil that rotates about an approximately vertical axis, as that supporting a helicopter or autogiro in flight;

c) Unmanned Aircraft Systems (UAS): an unmanned aircraft (UA), commonly known as a drone, is an aircraft without a human pilot on board. Its flight is either controlled autonomously by computers in the vehicle, or under the remote control of a pilot on the ground or in another vehicle. UAS can either be fixed or rotary wing craft; and may be operated singly or in swarms (communicating with each other and with the ground under centralized control) or

[3] Cf. the European Integrated Administration and Control System (IACS) <http://ec.europa.eu/agriculture/direct-support/iacs/index_en.htm> aimed at preventing fraud in agricultural subsidies. IACS includes satellite surveillance.

[4] A different categorization appears on page 2 of Stanley, J and Crump. C., „Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft“, ACLU Report dated December 2011 (available online at http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf)

d) Other: an aerostat is a craft that remains aloft primarily through the use of buoyant lighter than air gases, which impart lift to a vehicle with nearly the same overall density as air. Aerostats include free and/or moored balloons, airships or dirigibles and may be powered or unpowered.

Each of these platforms will have different operating characteristics such as operating altitude, speed, range, endurance (i.e., how long can the platform remain aloft), ability to loiter, and payload capacity.

Surveillance Technologies

A variety of surveillance technologies can be carried by the above-mentioned platforms, the exact payload being dependent on a number of factors including mission, weather, payload capacity, the range of the sensor, its field of view and resolution, and so on. Sensors include (but aren‘t necessarily limited to):

a) Visible spectrum: these sensors are typically in the form of cameras, including high-definition and full motion video systems[5]; they allow for continuous live surveillance and storage of the entire video footage;

b) Infra-Red (IR): these types of sensors detect energy emitted or reflected from the target. Most IR sensors are passive, although they may be used in conjunction with an IR illumination source. They can „see“ through smoke, fog, haze and other atmospheric obscurants better than a visible light camera;

c) Night Vision: the ability to see in low light conditions, based on a combination of sufficient spectral range (i.e., how much of the electromagnetic (EM) spectrum the device can detect) and sufficient intensity range (i.e., how much light is needed to form a useful image). Night vision technologies can be broadly divided into three main categories:

   1. Image intensification: these technologies work on the principle of magnifying the amount of received photons from various natural sources such as starlight or moonlight. Examples of such technologies include night glasses and low light cameras;

   2. Active illumination: these technologies work on the principle of coupling imaging intensification technology with an active source of illumination in

[5] The U.S. Army recently acquired a 1.8 gigapixel camera for use on its drones. This camera (Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System – ARGUS IS) offers 900 times the pixels of a 2 megapixel camera found in some cell phones; it was built at low cost using 368 camera chips from cell phones. It can track objects on the ground 65 miles away from an altitude of 20,000 feet. Cf.*US Army unveils 1.8 gigapixel camera helicopter drone*, BBC NEWS (29 December 2011), http://www.bbc.com/news/technology-16358851. An instructive video can be seen at: http://www.youtube.com/watch?v=QGxNyaXfJsA> accessed on 2 April 2013.

the near infrared (NIR) or shortwave infrared (SWIR) band. Examples of such technologies include low light cameras; and

3. Thermal imaging: these technologies work by detecting the temperature difference between the background and the foreground objects.

d) Radar: radar uses very high frequency radio waves to determine the range, altitude, direction or speed of an object. Radar can also be used to identify and track objects, such as vehicles, on the ground (using, for instance, Side Looking Airborne Radar (SLAR)); and

e) Specialized sensors: a range of specialized sensors (e.g., to detect traces of chemical, biological, nuclear, radiological and explosive materials; license plate scanners; acoustic sensors, etc.) can also be carried by aerial surveillance platforms.

Combinations of these sensor types can provide organizations with the capability to conduct aerial surveillance under almost any conditions.

Privacy Implications

There are a number of aspects of surveillance that raise privacy concerns, including the surveillance being hidden, intrusive, indiscriminate and/or continuous.[6] Although these aspectswere articulated in the context of electronic surveillance, they are also applicable to aerial surveillance:

a) Hidden: depending on size, operating altitude, sensor capabilities and so on, it may not be possible to detect aerial surveillance (either the platform itself or the sensors being used). Those subject to surveillance would have to rely on self-disclosure by the organization conducting the surveillance or disclosure by a third party. Those subject to hidden surveillance are less able to hold the organization conducting the surveillance accountable;

b) Intrusive: the range of possible operating conditions for aerial surveillance platforms and the capabilities of their associated sensors increase the intrusiveness of aerial surveillance (they can „see“ almost anything and everything);

c) Indiscriminate: aerial surveillance generally covers an area that includes individuals and activities that do not warrant being subject to surveillance, resulting in an over-collection of information; and

[6] Freiwald, Susan, “A First Principles Approach to Communications Privacy”, published in the Stanford Technology Law Review (2007 STAN. TECH. L. REV. 3), dated 2007. Available online at http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

d) Continuous: emerging aerial platforms combine increasing endurance and the ability to „stare“ at an area to effectively create continuous surveillance of any given area[7].

These characteristics give rise to some specific privacy concerns[8]:

a) Mission creep: although most people would likely support the use of aerial surveillance (e.g. for detecting and monitoring natural disasters), or for use in specific, limited law enforcement circumstances, it seems inevitable that other privacy-invasive uses would be found for such technology;

b) Tracking: the ability to maintain surveillance over an extended area for an extended period of time raises the possibility that individuals and vehicles could be tracked on an on-going basis;

c) Proliferation as the cost of UAS technology is rapidly falling. UAS may be bought or built by private individuals for use as “personal” or “DIY” UAS.

More privacy intrusive than CCTV

The privacy implications of CCTV have been a subject of debate for years, and many privacy authorities have issued guidelines on the necessary safeguards regarding its use. As explained above, aerial surveillance systems have the potential to be much more privacy intrusive than CCTV systems, for several reasons including:

- Aerial surveillance systems may use many more different sensors than CCTV systems.

- The installation of CCTV usually requires access to and control of the premises concerned, which is not required for aerial surveillance systems, in particular for outdoor locations.

- Depending on flight height and other factors (e.g. miniaturization) aerial surveillance systems may be more difficult – if not impossible – to detect by the persons observed than most CCTV systems.

[7] The U.S. Air Force has developed the “Gorgon Stare” technology, a spherical array of nine cameras fitted to a drone which is able to capture motion imagery of whole cities (“With Air Force’s Gorgon Drone ‘we can see everything’”, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html

[8] A discussion of different potential privacy concerns/issues appears on page 11 of Stanley, J and Crump. C., “Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft”, ACLU Report dated December 2011 (available online at http://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf)

- Aerial surveillance systems may be deployed without any delay, not requiring installation or configuration on site.

This clearly indicates that the safeguards in place for CCTV, while indicating a minimal standard, cannot be considered sufficient in the context of aerial surveillance systems and have to be adapted and complemented by specific measures appropriate for the different aerial surveillance systems and usage scenarios.

Therefore certain new essential safeguards should be adopted by regulators on a national level taking into account possible differences between the public and the private sector. Furthermore, since aerial surveillance does not stop at national borders international agreements will be necessary to prevent a "global panopticon" from emerging.

Recommendations

Whether operated by law enforcement or other public sector agencies, by private sector companies, or flown recreationally by citizens, the increasing use of aerial forms of surveillance will likely intensify concerns about how to preserve and protect individual and collective privacy as people go about their daily lives. If aerial surveillance becomes an increasingly common fixture in today's society, and society accepts that presence as normal, it is conceivable that society's expectations of privacy in public could seriously erode. It is important to secure an appropriate balance between the needs of law enforcement, public safety, etc. on the one hand and the legitimate privacy interests of individuals on the other. With that in mind, the Working Group makes the following recommendations:

a) the use of aerial surveillance should be limited to specific purposes[9] (e.g., searching for missing persons, border surveillance, legitimate private purposes such as access to information by journalists);

b) the use of personal data such as images collected from the air by government agencies should require a judicial warrant;

[9] The ACLU describe the following constraints on the use of drones:
[a)] **USAGE LIMITS:** Drones should be deployed by law enforcement only with a warrant, in an emergency, or when there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific criminal act;
[b)] **DATA RETENTION:** Images should be retained only when there is reasonable suspicion that they contain evidence of a crime or are relevant to an ongoing investigation or trial;
[c)] **POLICY:** Usage policy on domestic drones should be decided by the public's representatives, not by police departments, and the policies should be clear, written, and open to the public; and
[d)] **ABUSE PREVENTION & ACCOUNTABILITY:** Use of domestic drones should be subject to open audits and proper oversight to prevent misuse.
See http://www.aclu.org/blog/tag/domestic-drones; see also the resources listed by EPIC at http://www.epic.org/privacy/drones mentioning several bills addressing these issues currently before the U.S. Congress.

c) to the maximum extent possible, the public should be notified about the use of aerial surveillance; this requires e.g. that any UAS with the ability to collect and transmit information over a data link reports a GPS location, capabilities and ownership (e.g., government agency, company or private individual responsible for the particular platform or vehicle), in real time, to a competent authority and that this authority makes location information available, as open data, in real time;

d) surveillance should be restricted to as confined an area as possible (by limiting sensor fields of view), in order to minimize the likelihood of „over-collection“;

e) stringent controls over how aerial surveillance information can be used and who has access to that information should be implemented. Exceptions can be made for emergencies (e.g., searching for missing persons); and

f) there should always be a „man in the loop“ so that if there are any problems or unusual circumstances (e.g., the UAS starts to drift into a residential area), these can be addressed in as timely a manner as possible.

In view of the rapidly evolving technology, the Working Group will continue to monitor developments in this field closely.