Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983 – 2006

International Documents on Data Protection in Telecommunications and Media 1983 – 2006

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: Druckerei Feller

Inhaltsverzeichnis / Contents

Einleitung / Introduction 10/11

A. Beschlüsse der Internationalen Konferenz der Datenschutzbeauftragten 13

Resolutions of the International Conference of Data Protection Commissioners 13

5. Konferenz, 18. Oktober 1983, Stockholm 13
Neue Medien 13

New Media 13

7. Konferenz, 26. September 1985, Luxemburg 14
Datenschutz und Neue Medien 14

Data Protection and New Media 15

9. Konferenz, 24. September 1987, Oslo 16
Neue Medien 16

New Media 17

11. Konferenz, 30. August 1989, Berlin 18
Berliner Resolution 18

Berlin Resolution 20

Entschließung über die Arbeitsgruppe Telekommunikation und Medien 21

Resolution about the Working Group on Telecommunications and Media 22

Beschluß zu ISDN 24

Resolution on Integrated Services Digital Networks (ISDNs) 25

12. Konferenz, 19. September 1990, Paris 27
Probleme öffentlicher Telekommunikationsnetze und des Kabelfernsehens 27

Resolution on Problems related to Public Telecommunication Networks and Cable Television 30

13. Konferenz, 4. Oktober 1991, Straßburg 34
Bericht der Arbeitsgruppe Telekommunikation und Medien über Probleme des Telemarketing, der Kartentelefone und der elektronischen Directories und Beschluss der Internationalen Konferenz der Datenschutzbeauftragten 34

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 38

14. Konferenz, 29. Oktober 1992, Sydney 42
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 42

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 51

28. Konferenz, 2. und 3. November 2006, London 60
Entschließung zum Datenschutz bei Suchmaschinen 60

Resolution on Privacy Protection and Search Engines 62

B. Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation: Gemeinsame Standpunkte, Memoranden und Arbeitspapiere 65

International Working Group on Data Protection in Telecommunications: Common Positions, Memoranda and Working Papers 65

Memorandum vom 12.11.1990 zum Vorschlag der EG-Kommission für eine ISDN-Richtlinie 65

Memorandum of 12th November 1990 on the Proposal of the EC Commission for a Council Directive on ISDN 68

Stellungnahme vom 6. Februar 1991 zum Artikel 19 des Vorschlags der EG-Kommission für eine allgemeine Datenschutzrichtlinie 72

Statement of 6th February 1991 on Article 19 of the Proposal of the EC Commission for a general Data Protection Directive 73

20. Sitzung, 15. und 16. April 1996, Berlin 73
Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet („Budapest – Berlin Memorandum“) 73

Report and Guidance on Data Protection and Privacy on the Internet ("Budapest – Berlin Memorandum") 84

Bericht und Empfehlungen zu Telekommunikation und Datenschutz im Arbeitsverhältnis (August 1996) 93

Report and Recommendations on Telecommunications and Privacy in Labour Relationships (August 1996) 105

Gemeinsame Erklärung über Kryptographie vom 12.September 1997 115

Common Statement on Cryptography of 12th September 1997 117

23. Sitzung, 14. und 15. April 1998, Hong Kong SAR, China 120
Gemeinsamer Standpunkt zu Datenschutz bei Suchmaschinen im Internet 120

Common Position on Privacy Protection and Search Engines 122

Gemeinsamer Standpunkt im Hinblick auf Invert-Suche in Teilnehmerverzeichnissen 124

Common Position relating to Reverse Directories 125

Gemeinsamer Standpunkt im Hinblick auf das Abhören privater Kommunikation 127

Common Position in relation to Interception of Private Communications 129

Gemeinsamer Standpunkt zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien im WorldWideWeb 130

Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the WorldWideWeb 131

25. Sitzung, 29. April 1999, Norwegen 132
Gemeinsamer Standpunkt zum Datenschutz bei Gebäude-Bilddatenbanken 132

Common Position on Data Protection Databases of Images of Buildings 134

Gemeinsamer Standpunkt zu intelligenten Software-Agenten 135
Common Position on Intelligent Software Agents 138

Gemeinsamer Standpunkt zur Sprechererkennung und Stimmerkennungstechnologien in der Telekommunikation 140
Common Position on Speaker Recognition and Voice Analysis Technology in Telecommunications 142

27. Sitzung, 4. und 5. Mai 2000, Rethymnon, Griechenland 144
Gemeinsamer Standpunkt zur Missbrauchserkennung in der Telekommunikation 144
Common Position on the detection of fraud in telecommunications 149

Gemeinsamer Standpunkt zu Infomediaries (Informationsmakler) – eine datenschutzfreundliche Geschäftsidee?“ 152
Common Position on Infomediaries – a privacy-friendly business model? 155

Gemeinsamer Standpunkt zu Datenschutz und Urheberrechts-Management 157
Common Position on Privacy and Copyright Management 160

Gemeinsamer Standpunkt zu Online-Profilen im Internet 163
Common Position regarding Online Profiles on the Internet 164

Gemeinsamer Standpunkt zu Datenschutzaspekten bei der Registrierung von Domain-Namen im Internet 164
Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet 168

Gemeinsamer Standpunkt zu Datenschutzaspekten der Veröffentlichung personenbezogener Daten aus öffentlich zugänglichen Dokumenten im Internet 171
Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet 171

28. Sitzung, 13. und 14. September 2000, Berlin 172
Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates 172

Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe 175

Gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz („Zehn Gebote zum Schutz der Privatheit im Internet“) 178

Ten Commandments to protect Privacy in the Internet World
Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements 180

29. Sitzung, 15. und 16. Februar 2001, Bangalore, Indien 181
Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten 181

Common Position on Privacy and location information in mobile communications services 184

30. Sitzung, 28. August 2001, Berlin 187
Arbeitspapier zu Datenschutz und internetgestützter Stimmabgabe bei Wahlen zu Parlamenten und anderen staatlichen Einrichtungen 187

Working Paper on Data Protection and Online Voting in Parliamentary and other Governmental Elections 189

Arbeitspapier zu Datenschutzaspekten digitaler Zertifikate und public-key-Infrastrukturen 191

Working Paper on Data protection aspects of digital certificates and public-key infrastructures 195

31. Sitzung, 26. und 27. März 2002, Auckland, Neuseeland 198
Arbeitspapier zur Überwachung der Telekommunikation 198

Working Paper on Telecommunications Surveillance 200

Arbeitspapier zum Schutz der Privatsphäre von Kindern im Netz: Die Rolle der elterlichen Einwilligung 202

Working Paper on Childrens' Privacy On Line: The Role of Parental Consent 206

Arbeitspapier zur Nutzung eindeutiger Identifikatoren in Telekommunikationsendgeräten: Das Beispiel IPv6 209

Working paper on the use of unique identifiers in telecommunication terminal equipments: the example of Ipv6 212

Arbeitspapier zur netzwerkbasierten Telemedizin 215

Working Paper on Web-based Telemedicine 220

34. Sitzung, 2. und 3. September 2003, Berlin 225
Arbeitspapier zu potentiellen Datenschutzrisiken im Zusammenhang mit der Einführung des ENUM-Service 225

Working Paper on potential privacy risks associated with the introduction of the ENUM service 227

Arbeitspapier zu Intrusion Detection Systemen (IDS) 229

Working Paper on Intrusion Detection systems (IDS) 234

35. Sitzung, 14. und 15. April 2004, Buenos Aires, Argentinien 238
Arbeitspapier zu Datenschutz bei der Verarbeitung von Bildern und Tönen in Multimedia Messaging Services 238

Working paper on Privacy and processing of images and sounds by multimedia messaging services 239

Arbeitspapier zu einem zukünftigen ISO Datenschutzstandard 241

Working Paper on a future ISO privacy standard 242

Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke 242

Working Paper on potential privacy risks associated with wireless networks 245

Arbeitspapier zu Meinungsäußerungsfreiheit und Persönlichkeitsrecht bei Online-Publikationen 248

Working paper on freedom of expression and right to privacy regarding online publications 249

36. Sitzung, 18. und 19. November 2004, Berlin 250
Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Online-Betrugs 250

Working Paper on Means and Procedures to Combat Cyber-Fraud in a Privacy-Friendly Way 256

Arbeitspapier zu Lehrplänen zur Internetsicherheit unter Berücksichtigung nationaler, kultureller und rechtlicher (einschließlich datenschutzrechtlicher) Anforderungen 261

Working Paper on Cyber Security Curricula Integrating National, Cultural and Jurisdictional (Including Privacy) Imperatives 263

37. Sitzung, 31. März und 1. April 2005, Madeira, Portugal 266
Zweites Arbeitspapier zum Datenschutz bei Online-Wahlen in Parlamentswahlen und Wahlen zu anderen staatlichen Gremien 266

Second Working Paper on Data Protection and Online Voting in Parliamentary and other Governmental Elections 268

38. Sitzung, 6. und 7. September 2005, Berlin 270
Arbeitspapier zu Web Browser Caching („Zwischenspeicherung") von personenbezogenen Daten bei öffentlichen Internet-Zugängen (z.B. Internet-Cafes) 270

Working Paper on Web browser caching of personal information in commercial and public multi-user web access environments (e.g. "Cybercafés") 272

39. Sitzung, 6. und 7. April 2006, Washington D. C., USA 273
Arbeitspapier zur Online-Verfügbarkeit elektronischer Gesundheitsdaten 273

Working Paper on Online Availability of Electronic Health Records 277

40. Sitzung, 5. und 6. September 2006, Berlin 280
Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP) 280

Working Paper on Privacy and Security in Internet Telephony (VoIP) 283

Trusted Computing, damit zusammenhängende Technologien zur digitalen Rechteverwaltung, und die Privatsphäre: Einige Fragestellungen für Regierungen und Softwareentwickler 286

Trusted Computing, Associated Digital Rights Management Technologies, and Privacy: Some issues for governments and software developers 289

Einleitung

Als der Berliner Datenschutzbeauftragte* 1980 zum ersten Mal Kollegen und Experten einlud, um die Konsequenzen der sogenannten „Neuen Medien“ für den Datenschutz zu diskutieren, tat er dies, um ein Forum für den informellen Austausch von Meinungen und praktischen Erfahrungen von Datenschutzbeauftragten aus verschiedenen Ländern zu einem Thema zu schaffen, das damals noch sehr spezialisiert erschien.

Dies war der Beginn der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation. 26 Jahre danach sind die Konvergenz von Medien und Telekommunikation und die Verarbeitung personenbezogener Daten in globalen Netzen – insbesondere im Internet – zu entscheidenden Bereichen geworden, in denen die Frage nach dem Datenschutz in der modernen Informationsgesellschaft zu beantworten ist. Die Internationale Arbeitsgruppe – oder „Berlin Group“, wie sie jetzt häufig genannt wird – ist zu einem Frühwarnsystem für die Beobachtung von Risiken technologischer Entwicklungen geworden, das gleichzeitig die Chancen einer datenschutzfreundlichen Netzarchitektur hervorhebt. Zu den Themen, die die Arbeitsgruppe frühzeitig behandelt hat, gehören Suchmaschinen, intelligente Software-Agenten, ortsbezogene Dienstleistungen und netzbasierte Telemedizin.

Diese Veröffentlichung enthält alle Dokumente, die von der Internationalen Arbeitsgruppe bis Herbst 2006 verabschiedet wurden. Sie werden ergänzt durch eine Reihe von Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten, die von der Arbeitsgruppe vorbereitet oder beeinflusst wurden. Die Artikel-29-Arbeitsgruppe der Europäischen Datenschutzbeauftragten hat ihrerseits bei verschiedenen Gelegenheiten Vorschläge der Internationalen Arbeitsgruppe aufgegriffen und unterstützt.

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

When the Berlin Data Protection Commissioner* in 1980 for the first time invited colleagues and experts to discuss the consequences of the so-called "new media" for the protection of privacy he did so to allow for an informal exchange of views and sharing the practical experience of Data Protection and Privacy Commissioners from different countries in what appeared then to be a specialised area.

This was the starting point for the International Working Group on Data Protection in Telecommunications. 26 years later the converging area of media and telecommunications and the processing of personal data in global networks – in particular the Internet – have become key sectors where the question how to protect privacy in the modern information society has to be answered. The International Working Group – or "Berlin Group" as it is now known – has developed into an early warning system monitoring risks arising from new technological developments but at the same time highlighting the opportunities of a privacy-friendly network architecture. Among the subjects which the Working Group addressed at an early stage were search engines, intelligent software agents, location-based services, web-based telemedicine.

This publication contains all documents adopted by the International Working Group until 2006. They are complemented by a number of resolutions passed by the International Conference of Data Protection and Privacy Commissioners which have been prepared or influenced by the Working Group. The Article 29 Working Party of European Data Protection Authorities has in turn on several occasions taken up and supported proposals made by the Berlin Group.

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. 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

internationale 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

telecommunication 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 sicherstel-

len 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 Ge-

schlecht (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 diesem 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 crimi-

nal 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 Regelungsrah-

men 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 individual (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.

B. 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 gespeichert 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 eine 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

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.

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 World-WideWeb 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 using

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, classifi-

cation 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 Messung 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 Privatsphäre 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:

a) Kontrolle,

b) Rückmeldung

c) Datensicherheit und

d) 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 Interna-

tional 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 telecomrnunications 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. *Öffentliche 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 pro-

tection 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 ak-

tuelle 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 Satelitten 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 systema-

tisch 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 Di-

rective 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 erle-

digen. 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 Hintergrundge-

räusche 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 erforderlich 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

1. 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.

2. 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.

3. 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.

4. 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 Soft-

[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]

ware 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 Privatsphäre 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 tttp://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 which could be used not only to prevent copyright infringements but also access

[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/

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 Do-main-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 per-

sonal 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 Convention 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 telecommunications 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 telecommunications 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 In-

terference" (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

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 zusätzlich unterstrichen worden durch den Gemeinsamen Standpunkt der Ar-

[1] Europäischer Gerichtshof für Menschenrechte, Fall Klass und andere, Entscheidung vom 18. November 1977, Serie A Nr. 28, S. 23

beitsgruppe 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 Entschei-

dung 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 online), 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 iternetworking", 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 Online 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] Oth-

[1] American Medical Association, "Guidelines for Medical and Health Information Sites on the Internet http://www.ama-assn.org/ama/pub/category/1905.html

ers may not be so sanguine. However, the growth in health information sites,[2] online 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 cook-

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

ies 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 vorzutäu-

[1] Siehe z. B. http://www.ENUM.org oder http://www.enum-forum.org für weitere Informationen.

schen."[2] 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.

---

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)

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 any

[2] The Belgian Data protection Authority has been specially active with this regard.

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

[*] Regarding their problems of jurisdiction Norway and Sweden were not able to support the document

cases 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 Ge-

[4] Z. B. kann ein Komplize ohne Vorstrafen dafür bezahlt werden, dass er seine Signatur für betrügerische Zwecke „verleiht".

schäften 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 Veröffentli-

chung „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 an-

erkannt 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 compo-

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*.

nents 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 tech-

[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.

nical security 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

[1] See <http://www.datenschutz-berlin.de/doc/int/iwgdpt/online_voting.htm>).

an 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 öf-

* Wegen Besonderheiten in der nationalen Gesetzgebung kann das Papier von Italien nicht mitgetragen werden.

fentlichen 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

* Due to national legislation Italy is not able to support the document.

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 Lebens-

[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>

zeit 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 wird. Diese Entscheidung soll die Möglichkeit der relevanten Gesundheits-

[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

dienste 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 Standardisa-

tion (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 ist,

---

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 unautorisierte 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.

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 guaran-

---

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>

teed 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 Tech-

[8] Cf. footnote 4 above

nologien 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.