

Deklaracja z Mauritiusa

w sprawie Internetu Przedmiotów

Balaclava, 14 października 2014 r.

Internet Przedmiotów jest i pozostanie z nami. Coraz więcej urządzeń jest podłączonych do Internetu i są one w stanie się ze sobą komunikować, przy czym często użytkownik nie jest świadomy takiej komunikacji. Urządzenia te mogą znacznie ułatwić nasze życie. Na przykład w sektorze opieki zdrowotnej, transportu i energii połączone urządzenia mogą zmienić sposób, w jaki działamy. Jednak Internet Przedmiotów może również ujawniać intymne informacje na temat tego, co robią i dokąd chodzą ich właściciele, poprzez czujniki, jakie zawierają.

Samostanowienie jest niezbywalnym prawem wszystkich ludzi. Rozwój osobisty nie powinien być definiowany tym, co biznes i rząd wie o tobie. Rozpowszechnienie Internetu Przedmiotów zwiększa ryzyko, że tak się stanie.

W związku z tym zgromadzeni rzecznicy ochrony danych i prywatności omówili możliwości Internetu Przedmiotów i jego konsekwencje podczas 36. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności odbywającej się w Balaclavie na Mauritiusie, w dniach 13-14 października 2014 r. Czterech mówców reprezentujących zarówno sektor prywatny, jak i środowisko akademickie, przedstawiło rzecznikom informacje na temat pozytywnych zmian, jakie Internet Przedmiotów może wnieść w nasze codzienne życie, oraz na temat zagrożeń. Mówcy podsumowali, co należy zrobić w celu zapewnienia dalszej ochrony naszych danych osobowych oraz naszego życia prywatnego.

Mająca następnie miejsce dyskusja doprowadziła do następujących spostrzeżeń i wniosków:

- Danych z czujników Internetu Przedmiotów jest wiele i charakteryzują się one wysoką jakością i wrażliwością. Oznacza to, że możliwe do wywnioskowania informacje są o wiele obszerniejsze i bardziej wrażliwe, a możliwość identyfikacji jest bardziej prawdopodobna niż nieprawdopodobna. Zważywszy na fakt, że możliwość identyfikacji oraz ochrona Big Data jest ogromnym wyzwaniem, oczywiste jest, że Big Data wygenerowane z Internetu Przedmiotów wielokrotnie zwiększają to

wyzwanie. W związku z tym takie dane należy uznać za i traktować jako dane osobowe.

- Choć wielu przedsiębiorstwom ten model biznesowy jest jeszcze nieznany, jasne jest, że wartość Internetu Przedmiotów tkwi nie tylko w samych urządzeniach. Pieniądze zarabia się na usługach związanych z Internetem Przedmiotów oraz na danych.
- Każda osoba żyjąca w dzisiejszych czasach zdaje sobie sprawę z faktu, że połączenie z siecią czy urządzeniami jest rzeczą powszechną. Może to dotyczyć w jeszcze większym stopniu osób młodych i przyszłych pokoleń, które nie mogą sobie wyobrazić świata bez takich możliwości komunikacji. Jednakże nie tylko oni powinni dbać o to, czy ich dane są chronione. Jest to wspólna odpowiedzialność wszystkich interesariuszy w społeczeństwie, tak aby utrzymać zaufanie do połączonych systemów. W tym celu kluczowa jest przejrzystość: oferujący urządzenia Internetu Przedmiotów powinni wiedzieć, jakie dane gromadzą, w jakich celach oraz jak długo dane te są zatrzymywane. Powinni wyeliminować pozakontekstowe niespodzianki dla klientów. Przy zakupie urządzenia lub aplikacji Internetu Przedmiotów klientowi należy zapewnić odpowiednie, wystarczające i zrozumiałe informacje. Obecne polityki prywatności nie zawsze zapewniają informacje w jasny, zrozumiały sposób. Zgody na podstawie takich polityk raczej nie można by uznać za świadomą zgodę. Przedsiębiorstwa muszą zmienić sposób myślenia, aby zapewnić, że polityki prywatności nie będą już służyły im jedynie do ochrony przed sporami.
- Przetwarzanie danych rozpoczyna się od momentu zebrania danych. Wszystkie środki ochrony powinny być dostępne już od samego początku. Zachęcamy do rozwoju technologii, które ułatwiają nowy sposób wprowadzania ochrony danych i prywatności konsumenta od samego początku. Ochrona prywatności w fazie projektowania (Privacy by design) oraz domyślna ochrona prywatności (Privacy by default) nie powinny już być traktowane jako coś osobliwego i powinny stać się kluczową cechą innowacyjnych technologii.
- Internet Przedmiotów stawia także znaczące wyzwania w zakresie bezpieczeństwa, którymi należy się zająć. Zwykła zaporą ogniową (firewall) już nie jest wystarczająca. Jednym ze sposobów minimalizacji zagrożenia dla osób jest zapewnienie, aby dane mogły być przetwarzane na samym urządzeniu (lokalne przetwarzanie). Gdy nie ma

takiej możliwości, przedsiębiorstwa powinny zapewnić szyfrowanie na całej drodze przesyłu danych, aby chronić dane przed nieuzasadnioną ingerencją.

- Organy ochrony danych i prywatności nadal będą monitorowały rozwój Internetu Przedmiotów. Zobowiązują się do zapewnienia zgodności z przepisami w zakresie ochrony danych i prywatności w swoich krajach, jak również z uzgodnionymi na poziomie międzynarodowym zasadami ochrony prywatności. W przypadku wykrycia naruszeń prawa, będą dążyły do odpowiednich działań w zakresie egzekwowania prawa, czy to samodzielnie czy też w ramach międzynarodowej współpracy.
- Biorąc pod uwagę ogromne wyzwania, przed jakimi stoją twórcy Internetu Przedmiotów, organy ochrony danych i osoby fizyczne, wszyscy interesariusze powinni zaangażować się w intensywną, aktywną i konstruktywną debatę na temat implikacji Internetu Przedmiotów i pochodzących od niego big data, aby podnieść świadomość na temat wyborów, których się będzie dokonywać.

Jacob Kohnstamm

Przewodniczący Komitetu Wykonawczego
Międzynarodowej Konferencji
Rzeczników Ochrony Danych i Prywatności

Drudeisha Madhub

Przewodnicząca
Urzędu Ochrony Danych
Mauritiusa