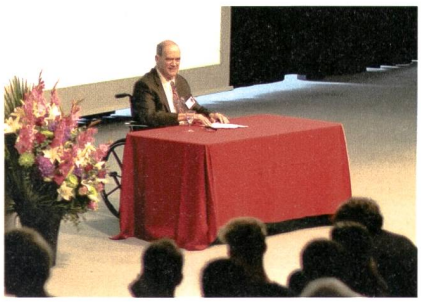
Die intransparente Transparenz digitaler Datenströme

Die intransparente Transparenz digitaler Datenströme

Congress on Privacy and Surveillance an der ETH Lausanne

Aus aktuellem Anlass, den öffentlich gewordenen Telekommunikations-Überwachungspraktiken, trafen sich rund 800 Interessierte am 30. September 2013 an der ETH Lausanne, deren Labor für algorithmische Kryptologie eingeladen hatte. Sieben Vorträge internationaler Experten beleuchteten nebst den technologischen Entwicklungen auch das Ausmass der Überwachung und stellten die zahlreichen juristischen Schwierigkeiten mit dem Datenschutz vor.



Bilder: No

Bill Binney, ein früherer technischer Direktor der NSA, gab Einblicke in deren System.

Radomir Novotny

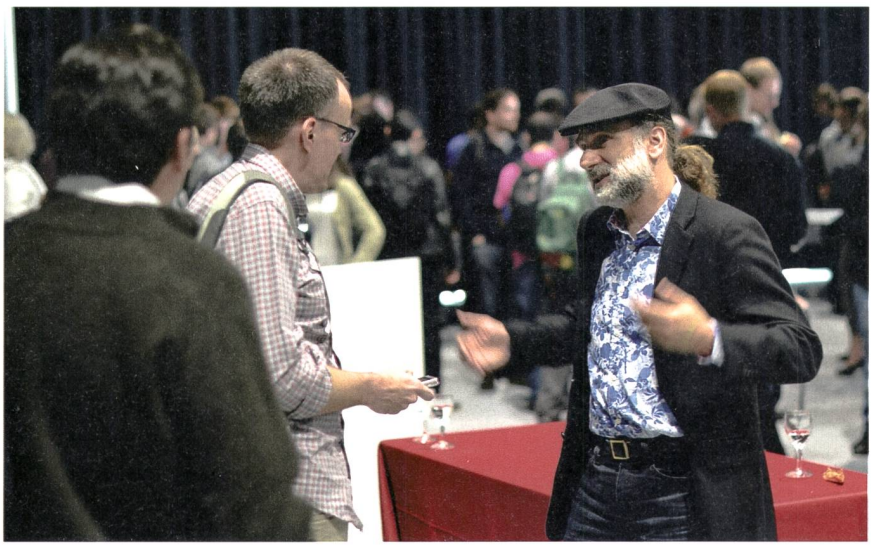
Die Enthüllungen von Ed Snowden bezüglich den Prism-, Upstream-, XKeyscore- und Bullrun-Programmen haben einiges ausgelöst. Zahlreiche Konferenzen in den Vereinigten Staaten zeugen davon, dass das Bedürfnis gewachsen ist, dem Datenschutz und der Überwachung nun auf den Grund zu gehen. Auch das europäische Interesse ist gross, denn die europäische Kommunikation läuft oft via USA – E-Mails und Telefonate wählen den billigsten und nicht den kürzesten Weg – und wird dort ohne Rücksichtnahme auf europäische Gesetzgebung abgehört, wie die Lausanner Tagung zeigte.

Obwohl die National Security Agency (NSA) in den Präsentationen einen wichtigen Platz einnahm, gingen gewisse Vorträge auch auf grundsätzlichere Fragen ein und beleuchteten die Thematik aus juristischer, technologischer und soziologischer Sicht.

Juristische Fragen

Aus rechtlicher Sicht gibt es gemäss Prof. Nikolaus Forgó, Leiter des Instituts für Rechtsinformatik der Uni Hannover, in der europäischen Datenschutz-Gesetzgebung zahlreiche Unklarheiten. Allein schon das Fehlen einer eindeutigen Definition von «privaten Daten» und von relevanten Präzedenzfällen schreckt vor langwierigen Rechtsstreitigkeiten ab – obwohl sich Juristen schon seit Jahrzehnten mit diesem Thema befassen. Es ist beispielsweise nicht klar, ob eine IP-Adresse, anonymisierte medizinische Daten oder Geoinformationen unter die privaten Daten fallen. Datenschutzbestimmungen sind deshalb oft vage und werden in EU-Ländern unterschiedlich implementiert. Das Einhalten der Bestimmungen lässt sich entsprechend schwer sicherstellen.

Ein weiteres Problem wird beispielsweise im Zusammenhang mit der NSA deutlich, die sich sozusagen in einem rechtsfreien Raum wähnt, da ihre Aktivitäten der nationalen Sicherheit dienen. Jeglicher, auch berechtigter, Widerspruch wird als Gefährdung derselben betrachtet. Die Verletzung individueller Menschenrechte stellt den Preis dar, der angeblich bezahlt werden muss, um das Ziel zu erreichen.



Der US-Kryptologe Bruce Schneier (r.) erläutert seine Sicherheitsthesen.

Der Whistleblower

Dass man der Sicherheit so einen Bärendienst erweist, zeigte der Whistleblower Bill Binney auf, der im Oktober 2001 nach 30-jähriger Arbeit, zuletzt als technischer Direktor, die NSA verliess. Sein fünfköpfiges Team entwickelte in den 1990er-Jahren das Projekt ThinThread, bei dem nur Daten, die mit verdächtigen Personen im Zusammenhang stehen, verschlüsselt gespeichert wurden. Nicht relevante Daten wurden ignoriert. Statt für dieses System entschied sich die NSA für Trailblazer, bei dem die Datenschutzmechanismen fehlen und sämtliche Daten unabhängig von ihrer Relevanz gespeichert werden. Binney stört sich an der Tatsache, dass dadurch das Missbrauchspotenzial erheblich stieg und dass die eigentliche Aufgabe, die Suche nach Gefahren, deutlich erschwert wurde.

Daten als Nebenprodukt

Eine ganzheitliche Position bezog der US-Kryptologe Bruce Schneier, der darauf aufmerksam machte, dass digitale Technologien immer sowohl erwünschte als auch unerwünschte Nebeneffekte mit sich bringen. Jede elektronische Kommunikation und Transaktion hinterlässt automatisch Spuren.

Ein erwünschter Nebeneffekt der Big-Data-Ansätze im kommerziellen Bereich sind die den Kunden anhand der erworbenen Produkte gemachten, möglichst nützlichen Kaufvorschläge. Unerwünscht ist aber der Einsatz dieser persönlichen Profile durch den Online-Dienst für andere Zwecke.

Gemäss Schneier soll man sich stets fragen, ob Aufwand und Ertrag in einem gesunden Verhältnis stehen. Im Falle des Sammelns von Daten könne dies zwar manchmal nützlich sein – beispielsweise beim Aufdecken von Kreditkartenbetrug, der im Vergleich mit terroristischen Anschlägen oft vorkommt und bei dem man die kritischen Muster kennt. Aber bereits 2006 schrieb Schneier in seinem Blog, dass dies zum Prognostizieren von terroristischen Anschlägen kein geeignetes Werkzeug sei, da sie sehr unterschiedlich organisiert bzw. durchgeführt werden. Man wisse sozusagen nicht, wie die Nadel aussieht, die man im gigantischen Heuhaufen suchen soll. Die Wahrscheinlichkeit für Fehlalarme sowie für nicht aufgedeckte Aktionen und der damit verbundene Kollateralschaden ist dabei hoch. Eine echte Erhöhung der Sicherheit bedingt ein sinnvolles, gezieltes Einsetzen des verfügbaren Budgets, statt dem Betreiben eines Systems, das zwar alles speichert, aber nur beschränkt fähig ist, Schlüsse aus den Daten zu ziehen.

Transparenz und Umdenken

Die auf juristisch wackligen Füssen stehende Datenschutzfrage beschränkt sich gemäss den Rednern nicht nur auf die NSA und auf die Nachrichtendienste anderer Länder, sondern betrifft auch kommerzielle Dienstleistungen wie Online-Shops und Cloud-Computing-Dienste, von denen manche beispielsweise über vertraglich vereinbarte Backdoors verfügen, die den nachrichtendienstlichen Datenzugriff vereinfachen. Auch die via Glasfaser übertragenen Telefondienste werden angezapft und Gespräche jahrelang gespeichert. Das Ausmass der Überwachung ist enorm und so eng mit dem Internet verbunden, dass nur aufwendige Verschlüsselungsmechanismen kombiniert mit Netzwerken zur Anonymisierung von Verbindungsdaten wie Tor («The Onion Router») eine einigermassen hohe Sicherheit versprechen.

Die Aufdeckungen Snowdens haben dem US-Kongress das Ausmass der NSA-Aktivitäten aufgezeigt. Dies könnte den Kongress zu empfindlichen NSA-Budgetkürzungen veranlassen. Zudem haben die Enthüllungen das Vertrauen in den Datenschutz renommierter US-Internetdienste erschüttert. Es ist noch nicht absehbar, ob diese neue Transparenz nachhaltige Veränderungen bewirken wird. Um wieder Vertrauen zu schaffen und den durch verunsicherte Nutzer ausgelösten Umsatzrückgang in Milliardenhöhe aufzufangen, ist die Kreativität der US-Internetfirmen gefragt.