Informationssicherheit

Überwachung in einer vernetzten Welt: Das Ende der Privatheit?

Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit
hannes.federrath@wiwi.uni-regensburg.de

Zusammenfassung

Junge Menschen wachsen heute selbstverständlich mit neuen technischen Möglichkeiten zur globalen Kommunikation und Interaktion auf. Doch erst das Wissen über Risiken und Chancen von Technik macht verantwortungsvolles Handeln möglich. Dazu gehört auch das Wissen über die Schutz- und Überwachungsmöglichkeiten, da Informationstechnik gleichermaßen für legale und illegale Zwecke eingesetzt werden kann.
An den Fallbeispielen Telefonüberwachung, biometrischer Reisepass, Autobahnmaut und Internet-Überwachung wird sichtbar, dass Überwachungs- und Kontrollmöglichkeiten oftmals wirkungslos bleiben oder die Freiheit des Einzelnen so stark einschränken, dass er sich auf Dauer unfrei fühlen muss.

Langfassung eines Beitrages in: Blick in die Wissenschaft, Forschungsmagazin der Universität Regensburg, 19 (2007) 18-24. Die gedruckte Version enthält nur wenige Literaturhinweise, diese dagegen alle Quellenangaben.

1 Neue Technik schafft neue Möglichkeiten

Die Sensibilität für den Datenschutz in der Wissensgesellschaft hat spätestens 1983 begonnen: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“ So formulierte es das Bundesverfassungsgericht in seinem „Volkszählungsurteil“ vom 15. Dezember 1983 [3]. Damals interessierte sich der Staat im Wesentlichen nur für die häusliche Situation seiner Bürger und deren Einkommen. Trotzdem war der Widerstand gegen die durchgeführte Volkszählung in der Bevölkerung groß.

In Zeiten von Payback-Karten, Google-Earth (Abb. 1) und der Allgegenwart von Videoüberwachung (privat wie staatlich) wirken die Bedenken der Verfassungsrichter noch aktueller als damals. Allerdings richten sich die Warnungen von Datenschützern und Bürgerrechtlern nicht

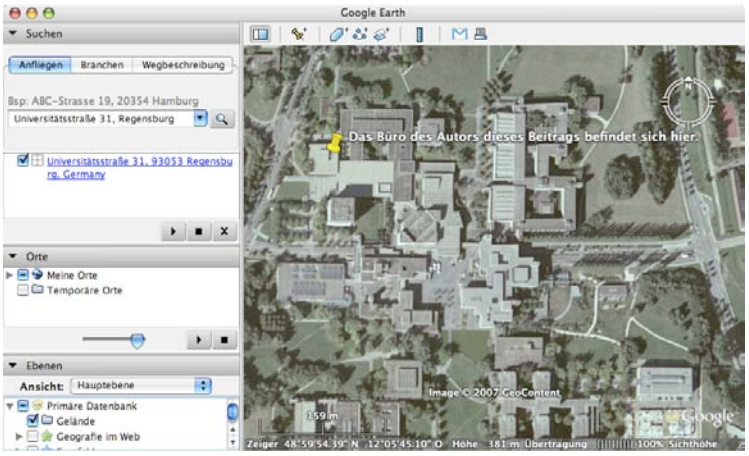

Abb. 1: Google Earth (http://earth.google.de) bietet für jedermann kostenlos detailreiche Bilder der Erde. Wohnlagen oder etwaige Urlaubsziele lassen sich so leicht selbst recherchieren.

mehr nur gegen den Staat, sondern vielmehr in erster Linie gegen global vernetzte Unternehmen und die private Sammelwut im Internet. Gleichwohl scheinen viele Bürger ihre persönlichen Daten heute bereitwilliger zur Verfügung zu stellen. In sog. Blogs (z.B. http://www.blog.de) werden öffentliche Tagebücher geführt, private Bildersammlungen sind weltweit abrufbar (z.B. http://www.flickr.com), und die viel genutzten Bonuskarten von Supermarktketten und Kaufhäusern versprechen geringste Rabatte als Gegenleistung für eine lückenlose Aufzeichnung des persönlichen Konsumprofils.

Nicht zwangsläufig sind neue Medien und Kommunikationsnetze gleichbedeutend mit neuer Überwachung. Technischer Datenschutz ist möglich. Privacy Enhancing Technologies ermöglichen einen Ausgleich der Interessen und helfen dem Einzelnen, sich vor Überwachung zu schützen. Verschlüsselungsprogramme wie Pretty Good Privacy (http://www.pgp.com) oder Gnu Privacy Guard (http://www.gnupg.org) sind heute leicht bedienbar und weit verbreitet. Privatheit beim Surfen schaffen Anonymisierungsprogramme wie TOR (http://tor.eff.org) und JAP (http://www.anon-online.org).

Auch in Zeiten globalen Terrors respektieren demokratische Staaten die informationelle Selbstbestimmung ihrer Bürger. So wurden beispielsweise Gnu Privacy Guard und JAP mit Bundesmitteln entwickelt. JAP (siehe auch Abschnitt 5) wurde maßgeblich an den Universitäten Dresden und Regensburg entwickelt und wird nach dem Ende der Projektförderung als Spin-Off weitergeführt (http://www.japtec.de).

Als Folge der Anschläge vom 11. September 2001 ist jedoch unverkennbar, dass die Überwachung der Bürger zunimmt, teilweise bedrohliche Ausmaße angenommen hat und oft alles Andere als zielführend ist. Aussagen wie „Das Internet ist kein rechtsfreier Raum.“ zeigen mangelndes Verständnis für die zugrunde liegende Technik und verdeutlichen die Ohnmachtserfahrung des Staates mit einer Kommunikationsinfrastruktur, die sich nationalstaatlicher Regulierbarkeit entzieht. Die Folge sind Forderungen nach immer besseren Überwachungs- und Kontrollmöglichkeiten, selbst dann, wenn sie wirkungslos bleiben werden oder die Freiheit des Einzelnen

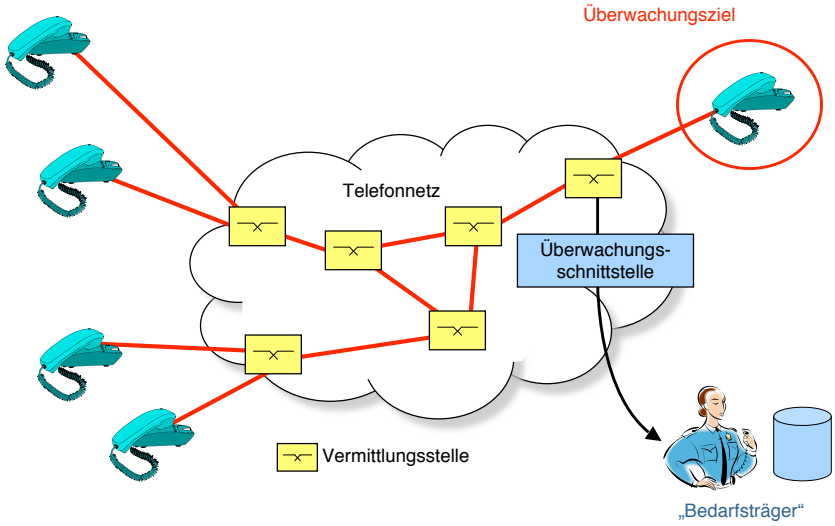

Abb. 2: Zur Telefonüberwachung wird dem Bedarfsträger nach richterlichem Beschluss in Echtzeit ein „Doppel“ (Kopie) der Gesprächsinhalte bereitgestellt.

stark einschränken. An den Fallbeispielen Telefonüberwachung, biometrischer Reisepass, Autobahnmaut und Internet-Überwachung soll dies im Folgenden gezeigt werden.

2 Telefonüberwachung

Zur Aufklärung und Verhinderung von schweren Straftaten, die im §100a der Strafprozessordnung in einem Katalog aufgezählt sind, darf ein Richter die Überwachung der Telekommunikation eines Betroffenen anordnen. Trotz des grundgesetzlichen Schutzes des Fernmeldegeheimnisses (Art. 10 des Grundgesetzes) dürfen auch Nachrichtendienste auf der Basis des sog. G-10 Gesetzes Telefongespräche mithören.

Technisch gesehen ist Telefonüberwachung heute sehr einfach. Dank der Digitalisierung des Telefonnetzes können die Netzbetreiber jederzeit zentral per Fernzugriff (Abb. 2) nahezu jede Vermittlungsstelle steuern und so die Gesprächsinhalte fast verzögerungsfrei dem sog. „Bedarfsträger“ (Polizei, Geheimdienst) übermitteln.

Die technische Richtlinie zur Telekommunikationsüberwachung [14] bestimmt die Zahl der gleichzeitig überwachbaren Telefonanschlüsse eines Netzbetreibers: Bei einem Netzbetreiber mit 10.000 Anschlüssen müssen dies knapp 50 sein, bei 100.000 Teilnehmern 134, bei einer Million Telefonkunden ist die gleichzeitige Überwachung von wenigstens 375 Anschlüssen vorzusehen. Genauer gesagt richtet sich die Zahl der überwachbaren Anschlüsse y in Abhängigkeit der Gesamtzahl x vorhandener Anschlüsse nach der Formel $y = 0,75 \cdot x^{0,45}$. Derart konkrete Vorgaben legen nahe, dass seitens der Bedarfsträger entsprechend viel Überwachungspersonal vorgehalten wird, um die Gespräche auch tatsächlich zeitnah zur Kenntnis zu nehmen. Erwähnt

sei noch, dass im Jahre 2004 in Deutschland etwa 55 Millionen Festnetzanschlüsse existierten und ca. 71 Millionen Mobilfunkanschlüsse [17].

Die tatsächliche Zahl von Telekommunikationsüberwachungen wird durch die Bundesnetzagentur in einer Statistik festgehalten. Im Jahre 2002 waren dies beispielsweise 21.874 Anordnungen. Nach Studien der Universitäten Bielefeld und Münster sollen auf der Grundlage dieser Anordnungen mehr als 20 Millionen Telefongespräche abgehört worden sein, wobei ca. 1,5 Millionen Bundesbürger (Ergebnis der Uni Bielefeld) bzw. sogar knapp 4 Millionen Bundesbürger (Ergebnis der Uni Münster) betroffen waren [19].

Ein Vergleich mit Zahlen aus den USA (ebenfalls entnommen aus [19]) verdeutlicht, dass die Größenordnung stimmt und offenbart zu dem, dass in Deutschland möglicherweise mehr überwacht wird als in den USA: Nach einer Statistik des Verwaltungsbüros der US-Gerichtshöfe wurden im Jahre 2005 von Bundes- und Staatengerichten 1773 Anordnungen erlassen und 625 von Bundesbehörden. Je Anordnung waren durchschnittlich 107 US-Bürger betroffen. Vergleicht man die Zahl der durchschnittlich betroffenen US-Bürger pro Anordnung mit der in Deutschland, wird deutlich, dass deutsche Gerichte möglicherweise sehr viel großzügiger bei der Telekommunikationsüberwachung sind: Bei geschätzten 1,5 bis 4 Millionen Betroffenen (Studien der Universitäten Bielefeld und Münster) und 21.874 Anordnungen waren bestenfalls 68 und schlimmstenfalls 182 Bürger je Anordnung betroffen. Bei 80 Millionen Bundesbürgern wird also schlimmstenfalls jeder 20. und bestenfalls jeder 53. Bundesbürger (zwischen 1,8 und 5 Prozent der Bevölkerung) wenigstens einmal pro Jahr abgehört.

Damit Bedarfsträger jederzeit die Zuordnung von Personen zu ihren Anschlüssen (und umgekehrt) herausfinden können, wurde im Telekommunikationsgesetz ein automatisiertes Auskunftsverfahren (genaue Bezeichnung: Schnittstelle für den Datenaustausch für das Auskunftsersuchen nach §112 Telekommunikationsgesetz zwischen der Regulierungsbehörde und den Verpflichteten, kurz: SARV) definiert, dessen Verwendung sich faktisch einer Kontrolle der ordnungsgemäßen und bedarfsgerechten Nutzung entzieht. Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können. Niemand, nicht einmal der Netzbetreiber, kann somit überprüfen, dass tatsächlich nur Zugriffe durch Strafverfolgungsbehörden erfolgen. Wo keine Zugriffsprotokolle geführt werden, lässt sich auch nicht die illegale Nutzung (durch organisiert Kriminelle oder Behördenmitarbeiter) feststellen.

Die im Mobilfunk zusätzlich vorhandene Möglichkeit der Lokalisierung eines Teilnehmers ist natürlich auch für die Strafverfolgung nützlich. Schon bald nach der Einführung der Mobilfunknetze wurde ein Gerät namens IMSI-Catcher entwickelt, das es ermöglicht, die Identitäten der in der Nähe befindlichen Mobiltelefone zu ermitteln (Abb. 3) und einzelne Telefongespräche mitzuhören.

Jeder Mobilfunkteilnehmer bekommt von seinem Netzbetreiber eine netzinterne Rufnummer (IMSI, International Mobile Subscriber Identity). Zur Identifizierung der in der Nähe befindlichen Teilnehmer sendet der IMSI-Catcher, den es mittlerweile in wenigstens zwei Ausführungen gibt (schwere Version für den Kofferraum und leichte Version, die in einen Rucksack passt), das Signal einer Basisstation aus und zwingt die Mobiltelefone zum Antworten mit ihrer IMSI. Bedarfsträger können mittels SARV leicht herausfinden, wem welche IMSI zugeordnet ist.

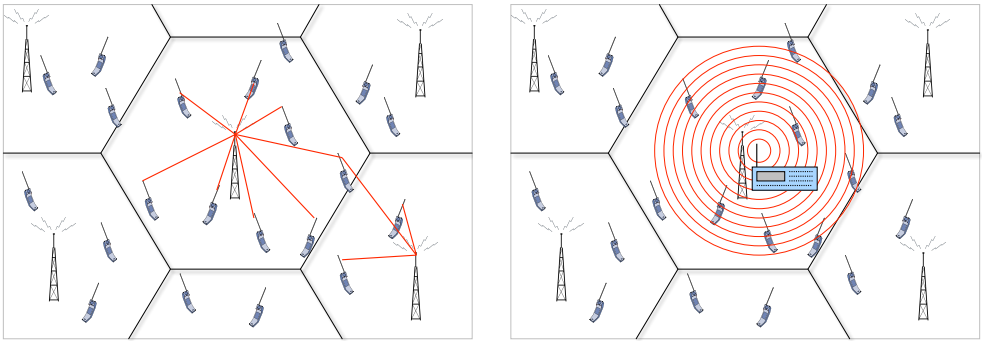

Abb. 3: Mobiltelefone melden sich bei der Basisstation mit dem besten Empfang an (links). Der IMSI-Catcher gibt sich als Basisstation aus und zwingt die Mobiltelefone zum Umbuchen (rechts).

Was den IMSI-Catcher so bedenklich macht, ist die Tatsache, dass alle in der Nähe befindlichen Mobiltelefone unbemerkt geortet werden, nicht nur die Telefone von Kriminellen. Derartige Kollateralschäden sind somit vom unbescholtenen Bürger hinzunehmen.

Der IMSI-Catcher wurde seit Mitte der 1990er Jahre von Polizei und Geheimdiensten ohne klare rechtliche Grundlage („rechtfertigender Notstand“) eingesetzt. Erst durch eine Änderung der Strafprozessordnung im Jahre 2002 wurde sein Einsatz im §100i legalisiert.

Allerdings wird nicht nur an Methoden zur Verbesserung der Überwachungsmöglichkeiten gearbeitet. Spätestens seit Mitte der 90er Jahre existieren Verfahren, die es ermöglicht hätten, die Lokalisierung der Mobilfunkteilnehmer und das Aufzeichnen von Bewegungsspuren zu verhindern. Verfahren zum Schutz vor Beobachtung von Telefongesprächen im Festnetz sind sogar schon seit Ende der 80er Jahre bekannt. Die verwendeten Methoden beruhen im Wesentlichen auf folgenden Ideen und wurden teilweise vom Autor mitentwickelt:

- Zur Verschleierung der Funksignale werden Sendeverfahren eingesetzt, bei denen das Mobiltelefon nicht auf einem schmalen Frequenzband sendet, sondern im gesamten Frequenzspektrum des Mobilfunknetzes. Solche Bandspreiztechniken können, wenn sie richtig eingesetzt werden, die Peilung eines Mobiltelefons vollständig verhindern, da seine Signale im spektralen Rauschen verschwinden. Hierzu muss das Signal mit einem Code moduliert werden, der dem natürlichen Rauschen sehr ähnlich ist [12].

- Soll niemand erfahren – auch der Netzbetreiber nicht –, wer mit wem kommuniziert, so muss dafür gesorgt werden, dass keinerlei Adressierungsdaten einen Personenbezug aufweisen. Üblicherweise werden die Inhaltsdaten, die zwischen zwei Teilnehmern ausgetauscht werden, nicht direkt gesendet, sondern über mehrere zwischengeschaltete Anonymisierstationen, die so die Kommunikationsbeziehungen verschleiern [11],[22].

- Die Aufenthaltsorte von Mobiltelefonen werden normalerweise vom Netzbetreiber in einer Datenbank gespeichert, damit ein eintreffender Ruf in die aktuelle Funkzelle weitergeleitet werden kann. Technisch gesehen ist es problemlos möglich, das Verfahren so zu

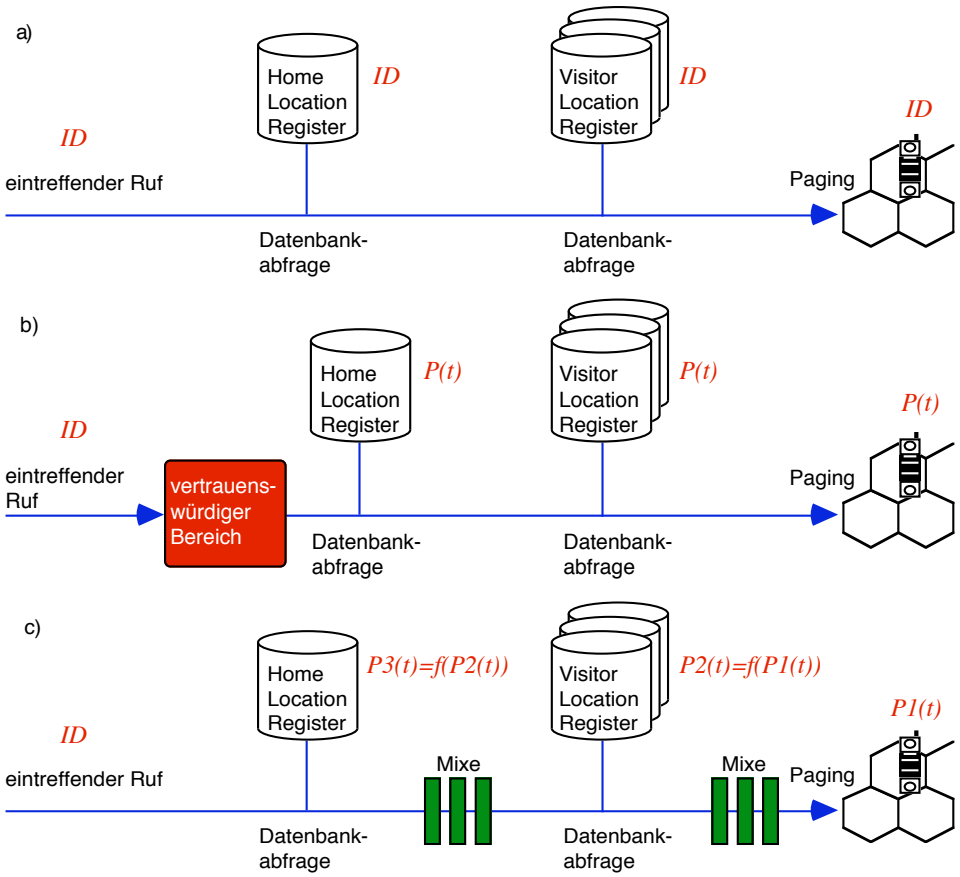

Abb. 4: Verbindungsaufbau a) bei GSM (heutiger Standard), b) bei der TP-Methode, c) bei den Mobilkommunikationsmixen

gestalten, dass auch der Netzbetreiber keinerlei Information darüber gewinnen kann, welche Kunden sich wo aufhalten. Mit Hilfe von Pseudonymen (Abb. 4), die auch für den Netzbetreiber nicht mit der Identität des Kunden verkettbar sind, gelingt dies sogar ohne signifikanten Aufwand [18],[9].

Obwohl die Möglichkeiten zum Schutz vor Beobachtung in Telekommunikationsnetzen gut erforscht sind, haben sie sich in der Praxis nicht durchgesetzt. Allerdings waren die Erkenntnisse sehr hilfreich für die Entwicklung entsprechender Verfahren für das Internet, wie im Abschnitt 5 gezeigt wird.

3 Biometrischer Reisepass

Seit Herbst 2005 wird zur Verbesserung der inneren Sicherheit der neue biometrische Reisepass eingeführt. Neben einem digitalisierten Foto, das über eine kontaktlose Schnittstelle ausgelesen

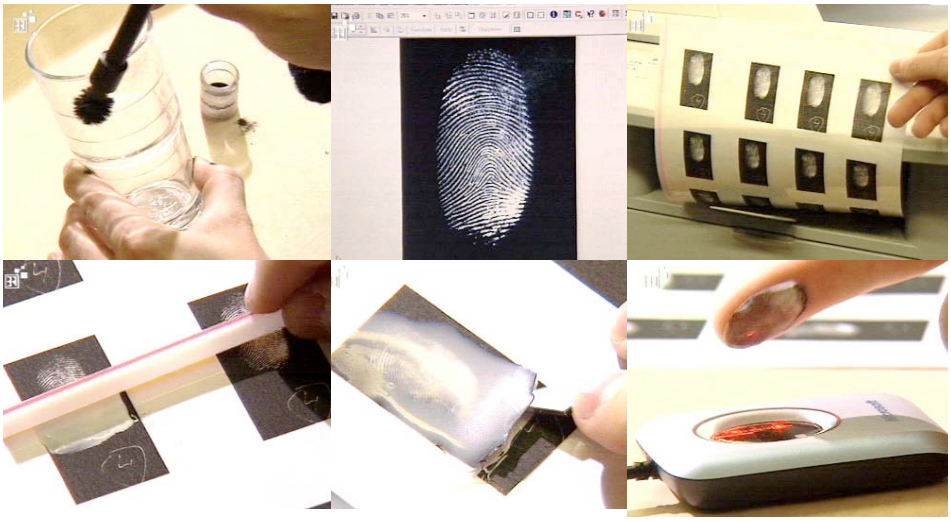

Abb. 5: Fälschen eines Fingerabdrucks: Fingerabdruck sichtbar machen, fotografieren, nachbearbeiten, ausdrucken, Leim auftragen, warten, abziehen.

werden kann, soll ab 2007 auch mit der Speicherung von Fingerabdrücken des Passinhabers begonnen werden. Diese zusätzlich gespeicherten Daten sollen die effizientere und zuverlässigere (sichere) Überprüfung der Identität von Personen ermöglichen. Leider wird das gewünschte Ziel jedoch nicht erreicht, wie im Folgenden gezeigt wird. Zudem bergen die neuen Daten das Risiko eines unautorisierten Zugriffs.

Seit einigen Jahren wird an der Nutzung biometrischer Merkmale zur zweifelsfreien Identifizierung von Menschen gearbeitet. Was in Hochsicherheitsbereichen bei einer überschaubaren Zahl von Berechtigten funktioniert, muss jedoch nicht zwangsläufig im Masseneinsatz tauglich sein, besonders dann nicht, wenn die eingesetzten Verfahren effizient sein sollen, also z.B. die Abfertigung an Grenzen beschleunigen sollen. Biometrische Daten, insbesondere wenn sie vom Auge abgenommen werden, können auch Auskunft über weitere Eigenschaften der Person geben, was deren Persönlichkeitsrechte verletzen kann [21]. Auch bei anderen biometrischen Merkmalen sind derartige „Sekundäreffekte“ nicht auszuschließen.

Hinsichtlich der Sicherheit zeigen Studien und Experimente [20, 24], dass viele der existierenden Verfahren für den Masseneinsatz zu unsicher sind. Einige Gesichtsscanner begnügen sich sogar mit einer zweidimensionalen Analyse der Gesichtsform bzw. einzelner Gesichtspartien und sind manchmal selbst durch das vorgehaltene Foto eines Berechtigten zu überlisten. Auch Fingerabdrücke (Abb. 5) lassen sich mittels Attrappen fälschen. Der Chaos Computer Club hat im Jahr 2005 gezeigt, dass zum Fälschen eines Fingerabdrucks wenig Ausstattung notwendig ist [5].

Die Vorgehensweise des Chaos Computer Clubs ist problemlos reproduzierbar, wie wir im Rahmen einer Fernsehsendung belegen konnten (siehe auch [13]): Der Fingerabdruck wird beispielsweise von einem Glas abgenommen. Ein „Detektivbaukasten“ aus dem Spielzeugladen enthält das notwendige Pulver zum Sichtbarmachen des Fingerabdrucks. Mit der Digitalkamera wird

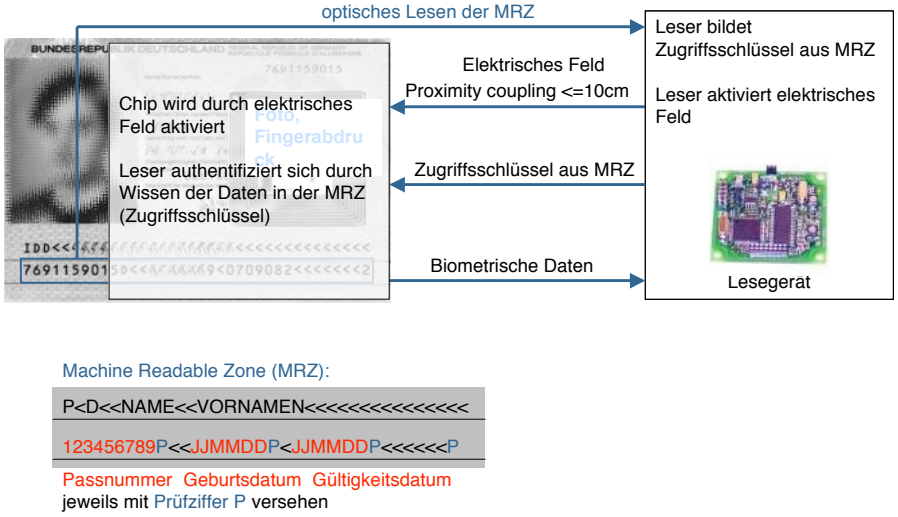

Abb. 6: Kontaktloses Auslesen der biometrischen Daten aus dem Reisepass (vereinfacht)

er abfotografiert und mit einem Bildbearbeitungsprogramm am Computer nachbearbeitet. Der Fingerabdruck wird mit einem Laserdrucker auf einer Folie ausgedruckt und anschließend mit Holzleim dünn überstrichen. Nach dem Antrocknen lässt sich der Toner gemeinsam mit dem Leim von der Folie abziehen und ist flexibel genug, eine „zweite Haut“ auf dem Finger zu bilden.

Sollen tatsächlich Grenzkontrollen mittels biometrischer Erkennungsverfahren sicherer werden, müssten Menschen (Grenzbeamte) sehr genau darauf achten, dass während der Erkennung keinerlei Manipulation möglich ist.

Abgesehen von der mangelnden Zuverlässigkeit biometrischer Erkennungsverfahren existiert beim biometrischen Reisepass ein relativ hohes Risiko, dass die gespeicherten Daten unberechtigt ausgelesen werden. Jeder biometrische Reisepass verfügt über einen Funkchip. Zur Aktivierung des Funkchips muss der Empfänger die Daten der sog. maschinenlesbaren Zone (Passnummer, Gültigkeitsdatum, Geburtsdatum des Passinhabers, Abb. 6) kennen. Jeder, der in den Pass sieht, kennt somit alle Daten zum Auslesen der biometrischen Daten und verfügt damit ggf. fortan über ein Digitalfoto des Passinhabers.

Das Alter einer Person lässt sich in relativ engen Grenzen schätzen; zudem werden (bzw. wurden) in manchen Ländern die Passnummern fortlaufend (bzw. systematisch) vergeben und korrelieren somit auch mit der Gültigkeitsdauer des Reisepasses, was den unberechtigten Zugriff auch ohne Kenntnis der maschinenlesbaren Zone möglich machen kann. Wenn Gültigkeitsdauer und Alter in einem Bereich von einigen Jahren liegen, sind zwar bis zu einige Milliarden Zahlenkombinationen durchzuprobieren (konkret etwa 2^{35}), ein normaler PC schafft dies jedoch problemlos innerhalb weniger Stunden [16].

Ab Herbst 2007 sollen auch Fingerabdrücke des Passinhabers gespeichert werden. Wenigstens hat man dort wegen der besonderen Sensibilität der Daten (biometrische Fingerabdruckdaten

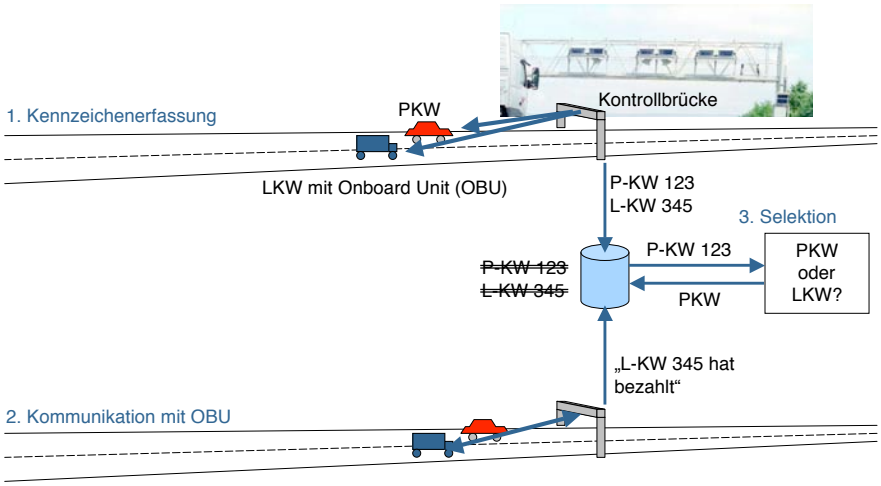

Abb. 7: Beim deutschen Autobahnmautsystem werden die Kennzeichen aller durchfahrenden Fahrzeuge vorsorglich erfasst.

unbescholtener Bürger könnten von organisiert Kriminellen ausgelesen werden, um sie anschließend an Tatorten als falsche Spuren zu „verteilen“) eine verbesserte Zugriffskontrolle vorgesehen, so dass wirklich nur Sicherheitsbehörden die Fingerabdrücke aus dem Pass auslesen können.

4 Autobahnmaut

Deutschlands Autobahnen verfügen über ein flächendeckendes Überwachungssystem zur Entdeckung von Mautprellern, das an den aufgestellten Kontrollbrücken zu erkennen ist. Das deutsche Mautsystem ist ein Prepaid-System für die Erhebung von LKW-Straßenbenutzungsgebühren. Um Betrug nachträglich feststellen zu können, werden alle durchfahrenden Fahrzeuge – sowohl LKW als auch PKW – fotografiert und deren Kennzeichen in einer Datenbank gespeichert. Fahrzeuge (LKW) mit einer Onboard Unit (OBU) tauschen Daten mit den Kontrollbrücken aus. Über die Onboard Unit wird die Straßenbenutzungsgebühr von einem Guthaben abgebucht. Fahrzeuge, die als PKW erkannt werden (bzw. für die keine Mautpflicht besteht), müssen sofort wieder aus der Datenbank gelöscht werden, während LKW gespeichert bleiben, wenn sie nicht bezahlt haben (Abb. 7).

Um den Datenschutzbedenken Rechnung zu tragen, die ein solches System aufwirft, wurde im Gesetz zur Erhebung der Autobahnmaut eine strenge Zweckbindung verankert. Die gespeicherten Daten dürfen nur zur Erhebung von Autobahnmaut verwendet werden. Trotzdem forderte der Generalbundesanwalt a. D. Nehm auf dem 44. Deutschen Verkehrsgerichtstag im Januar 2006, dass die Daten aus dem Mautsystem auch zur Strafverfolgung zur Verfügung stehen sollen. In der Praxis würde dies zu einem stetigen Verlust an informationeller Selbstbestimmung der Autobahnbenutzer führen: Zunächst würde man nur auf die dauerhaft im System gespeicher-

ten Daten zurückgreifen wollen (Mautpreller), später auch auf die zeitweise dort vorhandenen (z.B. LKW, die korrekt bezahlt haben), bis schließlich die bloße Erfassungsmöglichkeit aller Fahrzeuge (LKW und PKW) mit genauem Standort und Uhrzeit genügen würde, um deren Notwendigkeit auch für die Strafverfolgung zu begründen.

Die Betreibergesellschaft Tollcollect hat für die technische Realisierung dieses perfekten Überwachungssystems den Big Brother Award 2002 erhalten.

5 Internet-Überwachung

Geheimdienste und staatliche Einrichtungen mit Überwachungsbefugnissen überwachen heute auch das Internet. Über die in Deutschland eingesetzte Überwachungstechnik ist in der Öffentlichkeit wenig bekannt. Die bekanntesten von den USA betriebenen Überwachungssysteme sind Echelon und Carnivore, auf die im Folgenden beispielhaft eingegangen wird.

Echelon ist ein Satellitenüberwachungssystem, das Teil eines von der sog. UKUSA-Alliance betriebenen Überwachungssystems war. Die UKUSA-Alliance wurde 1947 gegründet. Ihre Existenz blieb bis 1999 geheim. UKUSA-Mitglieder waren die USA und Großbritannien, sowie als „Second Parties“ Kanada, Australien und Neuseeland. Später wurden Überwachungsabkommen mit „Drittländern“ abgeschlossen. Auch mit Deutschland gab es ein solches Abhörabkommen. Eine deutsche Echelon-Abhörstation steht in Bad Aibling [15, 23].

Die umfassende Aufklärung der Fähigkeiten des Echelon-Systems ist dem englischen Wissenschaftsjournalisten Duncan Campbell zu verdanken, der in seinem Bericht „Interception Capabilities 2000“ [4] viele Informationen über die Arbeit von Geheimdiensten zusammengetragen hat.

Das Echelon-System fängt die elektromagnetischen Strahlen internationaler Satellitenverbindungen mit eigenen Satellitenschüsseln auf, analysiert sie und vergleicht die übertragenen Daten mit Schlüsselwortlisten. In solchen Listen stehen nicht nur Wörter, sondern auch E-Mail-Adressen, Telefon-, Handy- und Faxnummern. Bei Bedarf wird dann die entsprechende Kommunikationsverbindung aufgezeichnet. Echelon erfasst nicht nur Satellitenkommunikation, sondern teilweise auch Funkverbindungen auf der Erde. Insoweit ist Echelon kein reines Internet-Überwachungssystem, allerdings werden heute viele Internetverbindungen im Fernbereich über Funk abgewickelt.

Spätestens nach dem Zerfall des Ostblocks suchten die UKUSA-Mitglieder nach neuen Einsatzmöglichkeiten für Echelon. Ein Bericht des EU-Parlaments aus dem Jahr 2001 über das Echelon-System kommt, was den Einsatz nach dem Ende des Kalten Krieges betrifft, jedenfalls zu dem Ergebnis, „[. . .] dass nunmehr kein Zweifel mehr daran bestehen kann, dass das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, [. . .]“ [25].

Es existieren aber auch speziell für das Internet geschaffene Überwachungssysteme. Carnivore ist beispielsweise ein vom amerikanischen FBI eingesetztes Werkzeug zur Überwachung des WWW- und E-Mail-Verkehrs verdächtiger Personen. Die Verwendung von Carnivore setzt eine

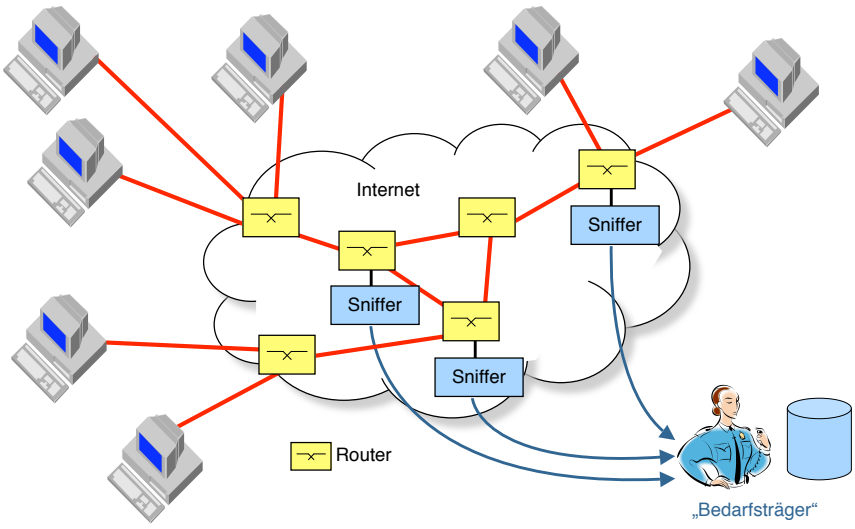

Abb. 8: Vergleicht man die Anwendung von Sniffern zur Internet-Überwachung mit der Telefonüberwachung, fallen kaum Unterschiede auf.

richterliche Anordnung voraus. Technisch ließe sich das System aber auch zur Rasterfahndung einsetzen.

Es wird „gespeist“ durch die für staatliche Stellen zugänglichen transferierten Kommunikationsinhalte von Internetnutzern (z.B. abhörbare Satellitenverbindungen) sowie durch gezieltes Abgreifen (z.B. beim Internet Service Provider des Überwachten) nach richterlicher Anordnung. Unter anderem dürften über das Echelon-System wesentliche Kommunikationsströme zur Überwachung beigesteuert werden, da eine Vielzahl von Internetverbindungen heute z.B. über Satelliten übertragen werden. Dies betrifft insbesondere internationale Kommunikationsverbindungen.

In einem Testreport des FBI [7] zur Leistungsfähigkeit wurde stolz berichtet, dass Carnivore in der Lage sei, „zuverlässig allen ungefilterten Internet-Verkehr auf einer Festplatte mitzuschneiden und zu archivieren.“ Dies betrifft aber offenbar nicht das ganze Internet, sondern lediglich die Kommunikationen einzelner zu überwachender Internet-Anschlüsse bzw. -nutzer. Die Überwachung des gesamten Internet-Verkehrs scheitert derzeit noch an mangelnder Speicherkapazität. So übertragen z.B. größere Unternehmen, die nicht einmal primär im Internet-Geschäft tätig sind, heute bis zu mehrere Terabyte (1 Terabyte entspricht 10^{12} Byte) monatlich über ihre Leitungen, Internet Service Provider kommen sogar auf mehrere tausend Terabyte pro Monat (siehe z.B. [1]).

Die Technik eines Überwachungssystems wie Carnivore besteht im Wesentlichen aus Netzwerk-Sniffern und einer sehr großen Datenbank (Abb. 8). Ein Sniffer ist eine Software, die alle z.B. bei einem Internet Service Provider durchgeleiteten Daten in Echtzeit analysiert. Vom Strafverfolger vorgegebene Filterkriterien könnten beispielsweise sein:

- Zeichne alle E-Mail-Sendungen von Absenderadresse *A* an Empfängeradresse *B* auf.

- Registriere alle WWW-Zugriffe von Nutzer X.
- Speichere alle Bits, die die IP-Adresse Y sendet und empfängt.

Vom Sniffer werden die interessanten Daten aus dem riesigen Datenstrom herausdestilliert. Da man nicht in jedem Fall wissen kann, welche der übertragenen Daten später einmal interessant sein könnten, werden die abgefangenen Daten ggf. in einer Datenbank gespeichert und stehen bei Bedarf zur späteren Analyse nach neuen Kriterien zur Verfügung.

Neben der ursprünglich speziell für Carnivore entwickelten Software werden heute vom FBI auch kommerzielle Sniffing-Tools eingesetzt [8].

Vergleicht man die Abb. 2 (Telefonüberwachung) und 8 (Überwachung im Internet) miteinander, fallen kaum Unterschiede auf. Dies ist auf die Konvergenz heutiger Kommunikationsnetze zurückzuführen. Die zugrunde liegenden Netzinfrastrukturen für Telefonie und Internet unterscheiden sich kaum noch. Selbst die angebotenen Dienste konvergieren mehr und mehr, wie man am Beispiel Voice over IP (VoIP) erkennen kann. Mit Diensten wie Skype (http://www.skype.com) können heute über das Internet auch Festnetz- und Mobiltelefone problemlos angerufen werden und SMS verschickt werden.

Diese Konvergenz hat jedoch auch ihre guten Seiten, was die Schutzmöglichkeiten betrifft: Während Schutzverfahren in Telekommunikationsnetzen von den Netzbetreibern implementiert werden müssen, jedoch aus Gründen, über die nur gemutmaßt werden kann, niemals umgesetzt wurden, lassen sich im Internet beliebige Sicherheitsanwendungen und Schutzsysteme ohne großen Aufwand realisieren. Dies führte schnell dazu, dass datenschutzfreundliche Selbstschutz-Werkzeuge entwickelt wurden.

Eines der wichtigsten Projekte zum Schutz vor Beobachtung im Internet entstand unter anderem mit Beteiligung der Universität Regensburg. Im Rahmen des Projektes „AN.ON – Anonymität Online“, das vom Bundeswirtschaftsministerium gefördert wurde, entstand die Software JAP, die es ermöglicht, anonym durch das Internet zu surfen [2, 10]. Das Anonymisierungsverfahren, das bei JAP eingesetzt wird, basiert auf dem sog. Mix-Verfahren von David Chaum [6].

Ein Mix ist eine Zwischenstation auf dem Weg einer Nachricht vom Sender zum Empfänger. Werden mehrere solcher Mixe in den Kommunikationsweg geschaltet, so verbergen sie die direkte Kommunikationsbeziehung. Surft beispielsweise ein Nutzer eine Internetseite an, so wird der Request verschlüsselt und über mehrere – wenigstens jedoch zwei – Mixe geleitet. Der erste Mix kennt zwar den Sender der Nachricht, weiß jedoch nicht, wohin die Nachricht geleitet wird. Der letzte Mix kennt den Empfänger, hat jedoch keine Information darüber woher der Request ursprünglich kam. Alle Mixe verarbeiten nur verschlüsselte Nachrichten und können somit auch den Nachrichteninhalt nicht lesen oder mit anderen Daten verknüpfen. Auf diese Weise ermöglicht ein Mix die Anonymisierung von Verbindungen und erfährt selbst noch nicht einmal etwas über die Kommunikationsbeziehungen. Wenn gleichzeitig viele andere Nutzer den Anonymisierer verwenden, sind sie in der Gruppe aller anonym (Abb. 9).

JAP anonymisiert heute monatlich etwa 6 bis 10 Terabyte Daten von Internetnutzern.

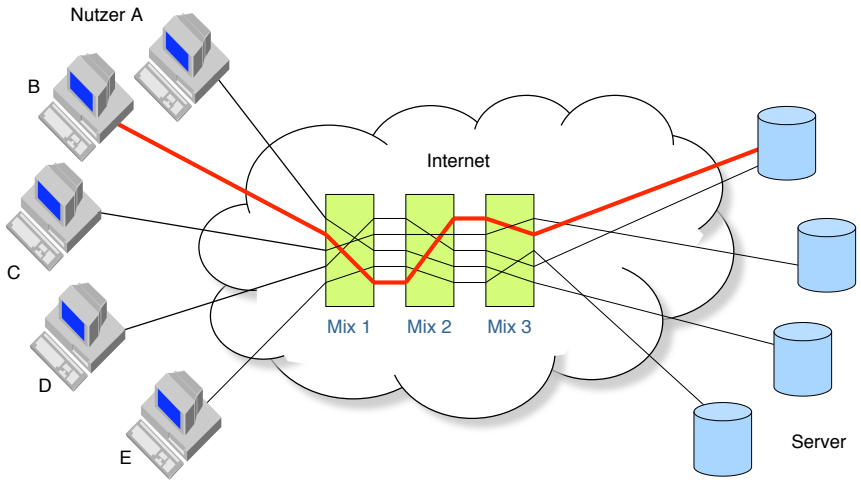

Abb. 9: JAP wird als lokaler Proxy im Browser konfiguiert, alle Webzugriffe gehen nun über die AN.ON-Server.

6 Schlussbemerkungen

Moderne Telekommunikationstechnik wird nicht nur zu legalen Zwecken eingesetzt, sondern kann auch missbraucht werden. Neben der Verabredung von Straftaten, Terrorakten und der Verbreitung illegaler Inhalte (z.B. Raubkopien, Kinderpornographie) können Kommunikationsnetze wie das Internet selbst zum Ziel krimineller Handlungen (z.B. Viren, Würmer, trojanische Pferde) werden, besonders dann, wenn sie sog. „kritische Infrastrukturen“ betreffen.

Dennoch darf die Privatheit nicht völlig dem Sicherheitsbedürfnis des Staates oder privater Organisationen untergeordnet werden. Die Annahme über sich selbst, „ich habe doch nichts zu verbergen“, führt hier nicht weiter. „Wenn Sie nichts zu verbergen haben, warum hat Ihre Toilette dann eine Tür, wo doch sowieso jeder weiß, was Sie dahinter tun?“ (frei nach einem Ausspruch eines Bürgerrechtlers auf einer amerikanischen Datenschutzkonferenz im Jahre 2000).

Auch in Zeiten von Terror gilt, was das Bundesverfassungsgericht schon 1983 formuliert hat: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. [...] Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“ [3] Umso wichtiger ist es, dass auch Techniken zur Verfügung stehen, die es dem Einzelnen ermöglichen, sich vor Beobachtung zu schützen. Mit den Forschungsarbeiten im Bereich Privacy Enhanced Technologies leisten wir hierzu unseren Beitrag.

Literatur

[1] 1&1 Internet AG: Rechenzentrum – Innovation und Technik für die Zukunft, 5.März 2007. http://www.1und1.de/index.php?&srcArea=ln&page=tech.

[2] Oliver Berthold, Hannes Federrath, Marit Köhntopp: Project "Anonymity and Unobservability in the Internet". In: Proc. Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000, Toronto/Canada, April 4–7, 2000. Association for Computing Machinery, ACM, ISBN 1-58113-256-5, 2000, 57–65.

[3] Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983. 1. BvR 209/83 Abschnitt C II.1.

[4] Duncan Campbell: Interception Capabilities 2000. The European Parliament. http://www.europarl.eu.int/stoa/en/publi/pdf/98-14-01-2en.pdf.

[5] Datenschleuder Nr. 87. Chaos Computer Club, 2005. http://chaosradio.ccc.de/media/ds/ds087.pdf.

[6] David Chaum: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84–88.

[7] FBI: FBI Carnivore Document, 5.Juni 2000. http://www.epic.org/privacy/carnivore/test_6_00.html.

[8] FBI: Carnivore/DCS-1000 Report to Congress, 18.Dez. 2003. http://www.epic.org/privacy/carnivore/2003_report.pdf.

[9] Hannes Federrath: Sicherheit mobiler Kommunikation. DuD Fachbeiträge. Vieweg, Wiesbaden, 1999.

[10] Hannes Federrath: Privacy enhanced technologies: Methods, markets, misuse. In: Proc. 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05), Lecture Notes in Computer Science 3592. Springer-Verlag, Berlin, 2005, 1–9. http://www-sec.uni-regensburg.de/2005/Fed2005TrustBus05InvitedPaper.pdf.

[11] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in Mobile Communication Systems: Location Management with Privacy. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 121–135.

[12] Hannes Federrath, Jürgen Thees: Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern. Datenschutz und Datensicherheit DuD 19/6 (1995) 338–348.

[13] Bayerisches Fernsehen: BR-Zeitspiegel. Sendung vom 11.5.2005 zur Biometrie in Reisepässen. http://www-sec.uni-regensburg.de/presse/biometrie_final.rm.

[14] Regulierungsbehörde für Telekommunikation und Post: Technische Richtlinie zur Beschreibung der Anforderungen an die Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜ). Ausgabe 5.0, Dezember 2006.

[15] Heise-News: Echelon-Lauschstation Bad Aibling wird geschlossen, 1.Juni 2001. http://www.heise.de/newsticker/data/fr-01.06.01-001/.

[16] Heise-News: ePass-Hack im niederländischen TV demonstriert, 2.Febr. 2006. http://www.heise.de/newsticker/meldung/69127.

[17] Christina Irion: Die Auskunfts- und Überwachungspflichten von Telekommunikationsdienstleistern nach dem TKG. Vortrag auf dem Datenschutzkongress des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V., Ulm, 17.März 2006.

[18] Dogan Kesdogan, Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Location management strategies increasing privacy in mobile communication. In: 12th International Information Security Conference. Chapman & Hall, London, Samos, Greece, 21.–24.Mai 1996, 39–48.

[19] Stefan Krempl: Kleiner Lauschangriff, ganz groß. ct 11 (2006). http://www.heise.de/ct/06/11/060/.

[20] Christian Meier: Biometrische Zugangskontrolle durch Gesichtserkennung. Diplomarbeit, Universität Regensburg, Institut für Wirtschaftsinformatik, Sept. 2006.

[21] Andreas Pfitzmann: Werden biometrische Sicherheitstechnologien die heutige IT-Sicherheitsdebatte vor neue Herausforderungen stellen? Ausgeladener Vortrag BSI-Kongress, 2005. http://dud.inf.tu-dresden.de/Literatur_V1.shtml.

[22] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead. In: Proc. Kommunikation in verteilten Systemen (KiVS), IFB 267. Springer-Verlag, Berlin, Febr. 1991, 451–463.

[23] Florian Rötzer: Lauschposten in Bad Aibling bleibt bestehen. Telepolis, 26.Okt. 2001. http://www.heise.de/tp/deutsch/special/ech/9937/1.html.

[24] Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler: Körperkontrolle – Biometrische Zugangssicherungen auf die Probe gestellt. ct 11 (2002) 114–123.

[25] Europäische Union: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)). EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon, Sitzungsdokument A5-0264/2001, Teil 1, 11. Juli 2001.

Über den Autor

Prof. Dr.-Ing. Hannes Federrath, geb. 1969 in Sonneberg/Thür. Studierte Informatik und promovierte 1998 an der Technischen Universität Dresden auf dem Gebiet der Sicherheit mobiler Kommunikation. Forschungsaufenthalte in Berkeley, Freiburg und Berlin schlossen sich an. Seit 2003 hat er an der Universität Regensburg den Lehrstuhl für Wirtschaftsinformatik mit dem Schwerpunkt „Management der Informationssicherheit“ inne. Er ist zugleich Vorsitzender des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD).

Forschungsgebiete: Datenschutzfreundliche Techniken, Sicherheit im Internet, Kryptographie, Mobile Computing, Digital Rights Management und Sicherheit im Electronic Commerce.