Context Aware Computing

Privacy Issues

Seminararbeit von

Alexander Bucher
und
Mark Furrer

Juni 2006

Inhaltsverzeichnis

1 Einleitung

1.1 Definition

Der Begriff „Privacy“ übersetzt man im Deutschen am Besten mit „Privatsphäre“. Das Verständnis von Privatsphäre hat sich über die Jahre hinweg geändert und wird gerade in jüngster Zeit wieder neu definiert. Eine der ersten Definitionen von Privatsphäre stammt wohl von Samuel Warren und Louis Brandeis aus dem Jahre 1890 und ist noch ziemlich einfach. Nach ihnen ist Privatsphäre *„the individual's right to be let alone“*[1], also das Recht eines jeden Individuums, in Ruhe gelassen zu werden.

Aktuellere Definitionen kreisen den Begriff einiges enger ein. So zum Beispiel Robert E. Smith (2000): *"[…] the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves”*[2]. Diese Definition teilt den Begriff der Privatsphäre in zwei Aspekte auf. Einerseits Umfasst sie das Recht auf unmittelbaren physischen Raum, in dem insbesondere die Intimsphäre des Menschen gewahrt bleibt. Dies entspricht ungefähr dem Sinn der herkömmlichen Definitionen. Neu ist jedoch der zweite Teil. Dieser umfasst das Recht der Individuen, alleinig über den Umfang der Informationen zu bestimmen, die sie über sich selber preisgeben. Somit ist die Problematik der Privatsphäre eng mit der des Datenschutzes verknüpft.

1.2 Gründe der Problematik

Die Problematik des Sammelns von Daten von und über Personen hat sich besonders in jüngster Zeit verschärft. Das rasante Tempo der technischen Entwicklung hat teilweise nicht nur die Gesetzesgeber überfordert. Als wichtigste technische Veränderungen sind zu nennen:

Vernetzung: Sie ermöglicht das Zusammenfügen verteilter Daten zu einem umfassenden System. Die Vernetzung ist längst nicht mehr lokal beschränkt, sondern hat mit dem Internet ein globales Ausmass erreicht.

Einfache Datenerfassung: Technisch vereinfachte Abläufe bei der Datenerfassung ermöglichen die einfache Gewinnung neuer Daten. Zu nennen sind Techniken wie Barcodes oder neu RFID-Chips.

Günstige Speichermedien: Sie ermöglichen ein dauerhaftes Aufbewahren dieser Daten über einer unbestimmten Zeitdauer. Modernen Datenbanken sind dadurch kaum Schranken gesetzt, was die maximale Kapazität gespeicherter Daten betrifft.

Rechenleistung: Mit heutigen leistungsstarken Computern lassen sich enorme Datenmengen innerhalb sinnvoller Zeit bearbeiten und auswerten.

1.3 Context Aware Computing

Entwickler und Erfinder neigen dazu, Datenschutz als eine „Sache für Juristen“ zu betrachten, die sie selber nicht betrifft. Für sie gibt es oft keinen Grund, sich etwa Gedanken über neuartige Definitionen der Privatsphäre zu machen. Im Vordergrund steht für sie grundsätzlich das Vorantreiben der Technologie. Der offensichtliche Nutzen der meisten Anwendungen des „Context Aware Computing“ ist dabei auch kaum von der Hand zu weisen: Unterstützung der Benutzer in fast allen Lebenslagen. Die Liste der möglichen Umsetzungen ist bereits heute schon ziemlich lang und potenzielle Benutzer finden sich sowohl im Baby- als auch im fortgeschrittenen Seniorenalter. Diese beiden Alterskategorien haben oftmals eines gemeinsam: Sie können nicht vollständig für sich selber sorgen. Deshalb müssen ihre Tätigkeiten von rational handelnden Menschen oder – auf längere Sicht gesehen günstigeren – Computern überwacht werden.

Aber auch vollständig mündige Personen lassen sich teilweise gerne überwachen. Diesen Eindruck könnte man fälschlicherweise gewinnen, betrachtet man die freiwillig verwendeten Hilfsmittel und Geräte dieser Kategorie von Personen aus einer datenschutzkritischen

Perspektive. Freizügig werden Informationen über seinen momentanen Standort preisgegeben oder man gestattet grossen Unternehmen einen intimen Einblick in seine persönlichen Einkaufsgewohnheiten. Die Wurzel des Problems liegt im grundlegenden Konzept des Context Aware Computing: Diese Art der Technik zielt in jeder seiner Anwendungen darauf ab, den Benutzer zu unterstützen und zwar abhängig vom gesamten Kontext, in dem sich der Benutzer befindet. Der Kontext schliesst hierbei sowohl die Umwelt des Benutzers als auch den Benutzer und seinen eigenen Zustand mit ein. Um entsprechende Entscheidungen treffen zu können, muss das System also per Definition zuerst den Kontext des Benutzers erfassen. Dazu bedienen sich die Systeme verschiedener Methoden. Sie alle haben jedoch zwei Dinge gemeinsam: Erstens braucht es einen Informationsfluss in Richtung des Systems, es müssen also Daten erfasst und verarbeitet werden. Zweitens gilt die Faustregel: Je mehr Informationen fliessen, umso genauer kann der Kontext modelliert werden. Eine automatische und möglichst effiziente Datenerfassung ist also zwangsweise Bestandteil eines jeden Context Aware Computing Systems.

Das Hunger der Context Aware Systemen nach möglichst vielen Informationen grenzt in nicht wenigen Fällen an eine völlige Transparenz der betroffenen Personen. Und nicht selten sind sich die Betroffenen nicht darüber im Klaren, welche Daten über sie erhoben werden und wie diese verwendet werden. Auch neigen selbst mündige Benutzer dazu, sich keine Gedanken über den Schutz ihrer Persönlichkeit zu machen, wenn sie sich dadurch das Leben leichter oder sicherer machen können. Darüber, dass dem Komfort- oder Sicherheitsgewinn stets ein Verlust eines Teils der eigenen Privatsphäre entgegensteht, darüber wird gerne hinweg gesehen.

Wir möchten dem Leser zeigen, warum Datenschutz ein wichtiger Bestandteil des Persönlichkeitsschutzes ist und wie er eingehalten wird. Dazu gehen wir zuerst auf die rechtliche Situation in der Schweiz ein. In den darauf folgenden zwei Kapiteln möchten wir einige konkrete Beispiele aufzeigen, wo bereits heute uns vertraute und unterstützende

Systeme Daten im problematischen Bereich sammeln. Abschliessend stellen wir kurz einige Techniken dar, wie sich Benutzer zumindest im Internet vor übermässiger Informationspreisgabe schützen können.

2 Rechtliche Aspekte

2.1 Begriffabgrenzung

Als erstes möchten wir die Begriffe „Datenschutz“ und „Datensicherheit“ voneinander abgrenzen. Diese werden, wie unterschiedlich sie in ihrer Bedeutung auch sein mögen, oft miteinander verwechselt. Analog zum Regenschutz, der den Menschen *vor Regen* schützt, wird auch beim Datenschutz der Schutz des Menschen und nicht der Daten verstanden. Insbesondere soll ein Schutz in Bezug auf das Erlangen, Bearbeiten und Aufbewahren von Daten von Individuen durch Dritte errichtet werden. Als Analogie zum Grundgedanken kann man das Urheberrecht heranziehen. Dieses schützt den Schöpfer eines Werkes in seinen Rechten an diesem Werk. Der Verfechter des Datenschutzes sieht das Individuum als „Urheber“ all seiner Tätigkeiten und Gedanken und schützt die Rechte, Informationen darüber zu sammeln, zu bearbeiten oder aufzubewahren.

Datensicherheit auf der anderen Seite befasst sich mit dem Schutz von Daten vor dem Zugriff Unbefugter. Hierbei stehen vor allem technische Aspekte im Vordergrund. Kernfragen der Datensicherheit befassen sich mit dem Sicherungsort von Daten, der Mechanismen der Zugriffskontrollen und Berechtigungsprüfungen als auch dem Schutz vor Verlust von Daten, beispielsweise durch defekte Hardware. Sobald man es mit der Aufgabe zu tun hat, Datensammlungen in einem geschützten Umfeld zu bearbeiten und aufzubewahren, befindet man sich in dem Bereich, in dem Datenschutz und Datensicherheit aneinander greifen. Um diese Aufgaben zu lösen, greift man auf die von der Datensicherheit bereitgestellten Werkzeuge zurück. Ein paar praktische Werkzeuge für den Privatanwender möchten wir im letzten Kapitel vorstellen.

2.2 Übersicht

Das Datenschutzgesetz (DSG) ist in der Schweiz seit 1. Juli 1993 in Kraft. Allerdings ist es nicht das erste Gesetz, das sich mit der Problematik des Schutzes der Persönlichkeit auseinander setzt. Schon lange Zeit sind die Gesetze über das Amts- und Berufsgeheimnis in Kraft, die Beamte, Geistliche, Verteidiger und andere (darunter auch Studenten) zu Verschwiegenheit verpflichten (vgl. Art. 320, 321 StGB[a]). Der grundsätzliche Persönlichkeitsschutz findet sich ausserdem seit 1985 auch im schweizerischen Zivilgesetzbuch (Art. 28 ZGB[b]). Neu am Datenschutzgesetz ist der präventive Charakter. Im Gegensatz zu den konventionellen Gesetzen setzt das Datenschutzgesetz schon weit vor einer möglichen Verletzung der Persönlichkeit an, während die bis anhin bestehenden Gesetze erst angewendet werden konnten, nachdem eine Rechtswidrigkeit stattgefunden hatte. Das schweizerische Datenschutzgesetz wurde, im Vergleich zu anderen westlichen Ländern, eher spät eingeführt. Seine Anwendung ist nicht auf private – also natürliche und juristische – Personen beschränkt, sondern erstreckt sich auch über die Bundesorganebene[c].

Im ersten Artikel des DSG wird der Zweck des Gesetzes festgelegt:

---

[a] **Art. 320, Abs. 1 Strafgesetzbuch (StGB):** Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Gefängnis oder mit Busse bestraft. […]
Art. 321, Abs. 1 StGB: Geistliche, Rechtsanwälte, Verteidiger, Notare, nach Obligationenrecht229 zur Verschwiegenheit verpflichtete Revisoren, Ärzte, Zahnärzte, Apotheker, Hebammen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist, oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Gefängnis oder mit Busse bestraft.
Ebenso werden Studierende bestraft, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen. […]

[b] **Art. 28, Abs. 1 ZGB:** Wer in seiner Persönlichkeit widerrechtlich verletzt wird, kann zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen.

[c] **Art. 2, Abs. 1 DSG:** Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch
a) private Personen;
b) Bundesorgane.

Art. 1 DSG: *„Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden."*

Dabei zielt das Gesetz vor allem auf Datensammlungen über Personendaten ab. Die beiden Begriffe werden im DSG wie folgt definiert:

Art. 3, Ziffer g, DSG: *„**Datensammlung**: jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind"*

Art. 3, Ziffer a, DSG: *„**Personendaten** (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen"*

2.3 Die Beschaffung von Personendaten

2.3.1 Rechtmässige Beschaffung

Die Beschaffung von Personendaten darf nur rechtmässig erfolgen[d]. Daraus ergeben sich zwei denkbare Szenarien für die erlaubte Gewinnung von Personendaten:

a) Die betroffenen Personen erklären sich ausdrücklich damit einverstanden, dass Personendaten über sie erhoben werden dürfen. Namentlich geschieht dies durch ein schriftliches oder mündliches Einverständnis. Entsprechende Klauseln können auch indirekt an andere Verträge gebunden werden. Beispielsweise können Teilnehmer einer Preisausschreibung sich damit einverstanden erklären, dass ihre Adresse für Werbezwecke verwendet werden darf.

b) Die Beschaffung der Personendaten ist notwendig für die ordnungsgemässe Erfüllung eines Vertrages zwischen Privaten. Die betroffene Person muss in diesem Fall nicht ihr ausdrückliches Einverständnis für die Verwendung der benötigten Daten geben. Vielmehr erklärt sie sich beim Abschluss des Vertrages stillschweigend damit einverstanden, dass die andere Partei ihre Daten verwenden darf. Namentlich wird beispielsweise ein Arbeitgeber einiges an Personendaten über seine Angestellten

[d] **Art. 4, Abs. 1 DSG:** Personendaten dürfen nur rechtmässig beschafft werden.

führen. Unter anderem wird er die Adressen dazu verwenden, um den Angestellten ihre Lohnabrechnungen zukommen zu lassen.

Noch weitere Möglichkeiten zur rechtmässigen Beschaffung von Personendaten sind denkbar. Beispielsweise kann man sich unzählige Szenarien vorstellen, die die Beschaffung von Personendaten aus sicherheitstechnischen Gründen erzwingen. Die meisten dieser Fälle lassen sich bei genauerem Betrachten jedoch in die gleiche Kategorie, wie eben unter b) beschrieben, einordnen. An einigen Grossanlässen beispielsweise werden einzelne Personen durchsucht, um sicherzustellen, dass keine Waffen in die Menschenmenge eingeschleust werden. Auch hier fallen unter Umständen Personendaten an, eine Übersicht der persönlichen Gegenstände, die eine Person bei sich trägt, beispielsweise. In diesem Beispiel kann nicht von einer „rechtswidrigen Beschaffung" gemäss Art. 4, Abs. 1 DSG gesprochen werden, denn die Gründe der Durchsuchung sind vertretbar.[e] Durch die Teilnahme an dem Anlass erklären sich die Betroffenen stillschweigend mit einer möglichen Durchsuchung einverstanden, da sie sich bewusst sein müssen, dass diese bei Grossanlässen durchaus üblich ist.

2.3.2 Rechtswidrige Beschaffung und Grauzonen

Rechtswidrig ist die Beschaffung von Personendaten insbesondere dann, wenn sich die betroffene Person klar gegen die Aufnahme ihrer Daten ausspricht oder wenn dies gegen ihr Wissen geschieht.[f] Schwieriger zu beurteilen sind insbesondere Situationen, in denen das Datenschutzgesetz mit dem öffentlichen Sicherheitsbedürfnis kollidiert. Denn gerade die öffentliche Sicherheit wird in jüngster Zeit oft als Rechtfertigungsgrund genommen, um Personendaten zu beschaffen.

Beispiel USA: Seit den Terroranschlägen in den USA vom 11. September 2001 hat das *U.S. Department of Homeland Security (DHS)* die Einreisebestimmungen für Ausländer

[e] Da in diesem Beispiel die „beschafften Daten" nicht aufbewahrt werden, wäre die rechtliche Anwendung des Datenschutzgesetzes sowieso fraglich. Das Beispiel dient nur zur Illustration der Verhältnismässigkeit.

[f] **Art. 4, Abs. 3 DSG:** Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

enorm verschärft[3]. Seit 2004 werden von allen ausländisch Einreisenden digitale Fingerabdrücke von beiden Zeigefingern sowie ein digitales Foto erfasst. Oberstes erklärtes Ziel dabei ist eine „erhöhte Sicherheit für Bürger und Besucher". Schwieriger zu verstehen – nicht nur für Datenschützer – ist das im selben Dokument ebenfalls genannte Ziel „die Privatsphäre der Besucher zu schützen". Problematisch in dem genannten Beispiel ist die Frage, ob der Umfang der gesammelten Daten (Fingerabdrücke, Foto) dem erhofften Nutzen gegenüber verhältnismässig ist.

Beispiel nationale Hooligan-Datenbank: Ein sehr aktuelles Thema in der Schweiz ist die mögliche Einführung einer bundesweiten Datenbank über Hooligans[g]. Insbesondere mit Blick auf die kommende Europameisterschaft 2008, die in der Schweiz und Österreich ausgetragen wird und den jüngsten Ausschreitungen in der Schweiz bei Fussballspielen, wird die Einführung einer solchen Datenbank von vielen Stellen gefordert. Sie ist damit Bestandteil eines neuen Gesetzesentwurfes gegen Rassismus, Hooliganismus und Gewaltpropaganda[5]. Betroffenen Personen soll dadurch der Zugang zu Stadien verwehrt bleiben. Der Grundgedanke stösst zwar auf allgemeine Zustimmung, trotzdem äussert sich der Eidgenössische Datenschutzbeauftragte noch kritisch zum vorgeschlagenen Gesetzesentwurf. Beispielsweise seien die Voraussetzungen, unter denen eine Person in die Hooligandatenbank aufgenommen werde, ungenügend präzisiert[6]. Auch Mängel in der Präzisierung der Datenflüsse, die zwischen den Betreibern der Datenbank und Privaten stattfinden sollen, nennt er. Durch die Behebung dieser Ungenauigkeiten soll ein Missbrauch der Datenbank verhindert werden.

Beispiel schweizerische AHV-Nummer: Ebenfalls ein äusserst aktuelles Thema ist die schweizerische Versichertennummer (genauer: Alters- und Hinterlassenenversicherungsnummer, AHV-Nummer). Ihre Verwendung ist längst nicht mehr auf die obligatorische AHV beschränkt, sondern sie wird wegen ihrer Eindeutigkeit längst auch in vielen anderen Bereichen verwendet, um Personen eindeutig zu identifizieren. Da die alte AHV-Nummer jedoch einiges an Personendaten codiert, ist sie datenschutztechnisch

[g] Als „Hooligans" werden „notorische Gewalttäter bei Publikumsveranstaltungen" bezeichnet. Sie fallen insbesondere durch Vandalismus und Anwendung von Gewalt gegenüber anderen Personen auf.

nicht mehr haltbar. Dies ist mit ein Grund, warum sie ab 2008 durch eine neue, anonyme Nummer ersetzt wird.

Der Aufbau der alten AHV-Nummer wird hier kurz an einem Beispiel erläutert: *373.83.159.114*. Folgende Informationen können dabei von jedermann aus den einzelnen Ziffern hergeleitet werden:

373: Dreistelliger Code für die **Anfangsbuchstaben des Nachnamens** (373 steht für die Buchstabenfolge „FUR“)

83: letzten beiden Ziffern des **Geburtsjahres**

1: **Geschlecht** (männlich: 1 – 4, weiblich: 5 – 8) sowie das **Quartal**, in dem die Person geboren wurde (wobei bei Frauen die 5 dem ersten Quartal entspricht, 6 dem zweiten usw.)

59: **Geburtstag**, gezählt ab Quartalsanfang (hier: 1. Januar + 59 Tage = 28. Februar)

11: **Ordnungsnummer**, im Falle von identischen Stammnummern sowie **Nationalität**: Die zweite Ziffer ist für Schweizer 1 – 4, für Ausländer und Staatenlose hingegen wird 5 bis 8 verwendet

4: Prüfziffer

Für die vollständige Beschreibung des Aufbaus der AHV-Nummer wird auf die Literaturliste verwiesen[7].

2.4 Bearbeitung von Personendaten

Die Bearbeitung von Personendaten muss verhältnismässig sein[h]. Dazu gehört auch, dass nicht mehr Daten gesammelt werden dürfen, als für den angegebenen Zweck notwendig sind. Beispielsweise wäre die Erstellung eines Bewegungsprofils der Kunden eines Mobilfunkanbieters nicht verhältnismässig bezüglich der Erstellung der monatlichen Rechnung und somit gesetzeswidrig. Zusätzlich dürfen Personendaten nur zu dem Zweck bearbeitet werden, für den sie bei der Beschaffung angegeben wurden. Dies bedeutet, dass gegebenenfalls selbst unternehmensintern nicht auf Personendaten von verschiedenen

[h] **Art. 4, Abs. 2 DSG:** Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

Abteilungen oder Projekten zugegriffen werden kann, je nach dem, wozu die Daten beschafft wurden. Dies impliziert auch das Verbot der Weitergabe der beschafften Daten an Dritte – es sei denn, dass dies ausdrücklich bei der Beschaffung angegeben wurde. Die Weitergabe an Dritte zur Bearbeitung in dem Sinne, wozu die Daten bestimmt sind, ist jedoch erlaubt, zumindest noch zum jetzigen Zeitpunkt. Allerdings muss der Auftraggeber die korrekte Bearbeitung der Daten in diesem Falle sicherstellen[i].

Bei jeder Bearbeitung von Personendaten ist die Persönlichkeit der Betroffenen grundsätzlich zu schützen. Dies umfasst unter anderem die Richtigkeit der Daten – falsche Daten dürfen nicht bearbeitet werden[j]. Des Weiteren muss die Datensicherheit gewährleistet sein[k]. Auch die Weitergabe der Daten an Dritte ist untersagt[l].

2.5 Auskunftsrecht

Zur Wahrung der Interessen des Datenschutzes wird ein Eidgenössischer Datenschutzbeauftragter eingesetzt. Er führt ein Register aller von privaten Personen geführten Datensammlungen, für deren Bearbeitung keine gesetzliche Pflicht besteht und von welcher die betroffenen Personen keine Kenntnis haben. In dieses Register hat jede Person Einsichtsrecht[m].

Datensammlungen, die nicht im eidgenössischen Datenregister eingetragen werden müssen, unterliegen ebenfalls dem Auskunftsrecht. Dabei ist jede Person berechtigt zu wissen, ob und welche Daten über sie bearbeitet werden[n].

---

[i] **Art. 14, Abs. 1 DSG:** Das Bearbeiten von Personendaten kann einem Dritten übertragen werden, wenn
   a) der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selber tun dürfte und
   b) keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

Dieser Artikel wird voraussichtlich bei der nächsten Revision des DSG aufgehoben werden!

[j] **Art. 5, Abs. 1 DSG:** Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.

[k] **Art. 7, Abs. 1 DSG:** Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

[l] Weitere Regelungen sowie Rechtfertigungsgründe: Art. 12, 13 DSG.

[m] **Art. 11 DSG:** 1. Der Eidgenössische Datenschutzbeauftragte führt ein Register der Datensammlungen. Jede Person kann das Register einsehen. […]

[n] **Art. 8 DSG:** 1. Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.
2. Der Inhaber der Datensammlung muss ihr mitteilen:
   a) alle über sie in der Datensammlung vorhandenen Daten

3 Privatsphäre im Physischen Raum

3.1 Warum brauchen wir Privatsphäre?

Um das Recht auf unmittelbaren physischen Raum, in dem sich in erster Linie die Intimsphäre des Menschen abspielt, ein bisschen genauer anzuschauen, müssen wir uns zuerst fragen, warum der Mensch überhaupt das Bedürfnis hat, sich abzuschotten und gewisse Sachen vor anderen Menschen zu verstecken.

Es ist selbstverständlich, dass man nicht jedermann seine intimsten Details preisgeben will, doch es gibt auch noch eine beachtliche Grauzone, in der nicht ganz klar ist, ob man nun beobachtet werden darf oder nicht. Natürlich hängt die grösser dieser Zone vom subjektiven Empfinden des einzelnen ab.

Ein gutes Beispiel dafür sind prominente Schauspieler, Sport- oder Musikstars. Da die Fans grundsätzlich so viel wie möglich über ihre Idole in Erfahrung bringen möchten, werden diese von der Haustüre an auf Schritt und tritt verfolgt und beobachtet. Beim Aufkommen der Stars ist der Rummel ja meist neu und nicht mal so unwillkommen. Doch spätestens wenn jeder Schritt überwacht wird und jeder kleine Patzer zu einer grossen Story gemacht wird, platzt den meisten Prominenten der Kragen. So kommt es doch nicht selten vor, dass mal ein Star einen Fotographen angreift oder zurechtweisen will. Allerdings verhalten sich die meisten Fotographen zwar aufdringlich, aber legal. Da stellt sich die Frage, wie viel Information man denn preisgeben muss, wie viel Information man überhaupt geheim halten kann und was man freiwillig in Interviews über sich selber preisgibt.

---

b) den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.

[…]

5. Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen. […]

Für den „normalen“ Bürger ist es um einiges einfacher, Informationen für sich zu behalten. Natürlich beobachtet vielleicht ein Nachbar, wenn ich das Haus verlasse, doch spätestens nach zwei bis drei Hausecken kann niemand mehr genau wissen, wo man hingeht. Allerdings gibt es auch Situationen, in denen man gerne möchte, dass man geortet werden kann. Sei das nun irgendwo in der Grossstadt, indem man auf dem Handy angerufen werden kann oder sei es anhand eines Ortungsgerätes, wenn man vergraben unter einer Lawine liegt und auf Rettung hofft. Natürlich kann man auch herkömmlich einen Zettel hinterlegen, wo man hingehen wird, doch dann besteht immer noch die Möglichkeit, an einen anderen Ort zu gehen und die Information somit nutzlos zu machen.

3.2 Ortung von Personen

Mittlerweile gibt es einige Technologien, welche die Ortung von Personen um einiges vereinfachen. Das einfachste und weltweit verfügbare Ortungssystem ist das Global Positioning System (GPS). Es ermittelt anhand von vier Satelliten die Koordinaten des Empfängers und auch dessen Geschwindigkeit. Was ursprünglich fürs Militär entwickelt wurde, ist nun auch zivil im Einsatz: Sowohl in Autos, in der Seefahrt und auch im Vermessungswesen wird das GPS eingesetzt. Doch gerade auch im Context Aware Computing wird die Funktionalität des GPS vermehrt verwendet. Allerdings funktioniert es in Gebäuden und Tunnels erst seit kurzem und zwischen hohen Gebäuden kann es durch mehrfache Reflektion des Signals zu Ungenauigkeiten kommen. Der SPS (Standard Positioning Service) ist öffentlich verfügbar und ermöglicht eine Ortung mit einer Genauigkeit von ca. 15 Meter. Anhand des dem Militär vorbehaltenem PPS (Precise Positioning Service) und mit Hilfe des Differential-GPS (DGPS) ist eine Ortung bis zu 5 Metern möglich. Für die Ortung einer Person allerdings wird neben dem passiven GPS-Empfänger auch noch ein aktiver Sender benötigt, wodurch sich sehr gute Überwachungsmöglichkeiten bieten.

Viel einfacher eine Person zu orten ist durch das GSM (Global System for Mobile Communication), welches in kleine Unterzonen (1-2 km^2 in der Stadt; 5-10 km^2 auf dem

Land) unterteilt ist. Falls der Benutzer am Telefonieren ist, kann anhand vom Abstand zu den Antennen eine noch genauere Ortung erfolgen. Allerdings ist dem Träger des Handys jederzeit möglich, dieses abzustellen und so jegliche Ortung zu verhindern.

Für eine mehr lokale Ortung eignen sich wohl am besten die aufkommenden RFID Chips. Momentan werden sie zur Identifikation von Tieren, bei Grossverteilern oder für kontaktlose Lesung von Karten (z.B. Skipässe) verwendet. Allerdings lässt die mikroskopische Grösse sowie die immer geringer werdenden Herstellkosten einiges für die Zukunft hoffen. Man könnte z.B. Patienten anhand von implementierten Chips erkennen, Kassen in Grossverteilern wie Coop und Migros ganz ersetzen und auch die Lagerprozesse dadurch um einiges optimieren. Probleme ergeben sich dabei, dass jedermann die Daten auslesen könnte und die Daten beliebig lange verfügbar wären. Allerdings wurde an der „International Conference of Data Protection and Privacy Commissioners" am 20.11.2003 in Sydney vereinbart, dass der Konsument alle Daten löschen können muss, und den RFID Chip auf Produkten zerstörbar oder abschaltbar sein muss. Des weiteren hält man fest: "all the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology."[8]

Diese neuen Techniken lassen einige Hoffnungen für die Zukunft zu. Es gibt zum Beispiel die Möglichkeit mit GPS Systemen auf PDAs einen Kollegenkreis aufzubauen, wo man jederzeit sehen kann, wer sich wo befindet. Diese Technologie ist zwar noch nicht ganz markttauglich, es scheint jedoch realistisch, dass in fünf Jahren einige Handys mit GPS-Systemen ausgestattet sein werden und es so möglich sein wird, einander jederzeit zu orten.

3.3 Beobachtung von Personen im öffentlichen Raum

Währenddem wir uns bisher nur gefragt haben, wie man eine Person auffinden kann, ist die Frage, wie oft und wie genau man beobachtet werden kann, etwa von gleichem Interesse. In der Öffentlichkeit wird man nicht nur von den Mitmenschen beobachtet, sondern besonders

in Geschäften befinden sich schon fast überall Überwachungskameras, meistens natürlich aus Diebstahlschutz. Neuerdings liegt jedoch auch die Überwachung im öffentlichen Raum im Trend: Immer mehr Bahnhöfe, Hallen, Plätze, Flughäfen sowie auch Schulen werden überwacht, mit dem Hauptziel, verbrechen zu verhindern oder zumindest aufzuklären.

Es gibt auch noch Beobachtungsvarianten, welche noch unauffälliger sind: Satelliten, ausgerüstet mit den richtigen Kameras, können genaue Bilder der Erde erstellen. Die kommerziellen Radare kommen dabei allerdings nicht auf die Qualität derjenigen des Militärs, welche eine Auflösung von bis 10 cm und weniger erreichen können. Analysten behaupten sogar, dass das Erkennen von Autonummern möglich sei[9]. Als Beispiel dazu ein Ausschnitt aus Google Earth[10], welcher die Terrasse der Mensa der Uni Binzmühlestrasse erkennen lässt.

Da die Technologie ja bekanntlich nie stagniert, wird es in Zukunft auch noch grössere Satelliten mit besseren Objektiven geben und dann auch eine bessere Auflösung. Allerdings sind Satelliten halt teuer und aufwändig und deshalb kann dies auch noch ein paar Jahre

dauern. Die Frage, wer dann diese Informationen veröffentlichen darf und was gegebenenfalls auch als Beweismittel verwendet werden kann, bleibt eine Frage der Politik.

3.4 Beobachtung von Personen im Privaten Raum

All diese Beobachtungsvarianten sind eher für den öffentlichen Raum gedacht. Um in der wirklichen Privatsphäre beobachtet zu werden, wird es schon ein bisschen schwieriger. Doch die immer preiswerter, kleiner und benutzerfreundlicher werdende Technologie ermöglicht schon fast jedem Hausbesitzer, eine Überwachungskamera zu installieren, damit der Nachbar keine Äpfel vom Baum klaut. Die Kinder werden mit der „Night Vision“ Funktion beim schlafen überwacht und jedermann kann problemlos per Videokonferenz kommunizieren. Dadurch bieten sich natürlich auch Möglichkeiten, die Arbeitnehmer am Arbeitsplatz zu überprüfen. Ob dies dann jedoch legal ist hängt von der jeweiligen Gesetzgebung ab. Fakt ist, dass die Überwachung durch Videokameras immer einfacher wird, und durch die Mikroskopischen Grössen der Kameras auch vermehrt versteckt und somit Illegal eingesetzt werden können, was zu beachtlichen Einbussen in der Privatsphäre führen kann.

4 Datenschutz / Privatsphäre der Informationen

4.1 Die Punktesammler

Das im Moment aktuellste Beispiel dazu sind die Grossverteiler Migros und Coop. Seit einigen Jahren gibt es nun schon die Cumulus- und die Supercard, womit man den Kunden einige Prämien verspricht. Im Gegenzug bekommen die Grossverteiler alle Informationen über die Personen und ihr Einkaufsverhalten. Durch so genanntes Data-Warehousing und Data-Mining können diese Daten dann auch gezielt verwendet werden. Fragen über Verkaufsmengen, Einkaufspersönlichkeiten, und Korrelationen über den Einkauf mehrerer Produkte können ohne grossen Aufwand beantwortet werden. Ein Problem dabei ist nicht

einmal dass die Daten verwendet werden, sondern eher dass sich die meisten Leute gar nicht bewusst sind, dass die Einkaufsdaten so genau weiterverwendet werden.

Der neuste Trend sind nun die Kreditkarten der Grossverteiler. Um eine Kreditkarte zu erhalten müssen gewisse persönliche Daten wie Monatseinkommen preisgegeben werden. Theoretisch wäre es dann also möglich, die Einkaufsdaten mit den Vermögensdaten zu Korrelieren, herauszufinden welche Produkte sich welche Einkommensklassen leisten und man könnte sogar personalisierte Aktionen gestalten, um beim Kunden die volle Zahlungsbereitschaft auszunützen. Auch wenn diese Korrelationen im Moment noch nicht erlaubt sind, da die Kreditkartendaten von einer Unterfirma unterhalten werden, sind sie trotzdem vorhanden und die Möglichkeiten sind nah.

Laut Gesetz muss der Kunde mit der Aufnahme der Information einverstanden sein. Weder die Cumulus-Karte noch die Supercard sind obligatorisch und auch ohne Kreditkarten wird einkaufen ohne Probleme möglich sein. Allerdings locken die Prämien, welche für fast jeden Geschmack etwas Gutes bieten, was uns meistens dazu bringt, unsere Daten, ohne grosses Hinterfragen was damit gemacht wird, herauszugeben.

4.2 Die klassifizierten Daten

Die Grossverteiler sind jedoch bei weitem nicht die einzigen, welche Informationen über ihre Kunden erheben. Das eigentliche Problem stellen diejenigen Daten dar, welche man nicht gerade jedem Fremden mitteilen möchte. Ein Beispiel dafür ist das Vorstrafenregister. Der Staat hat ein Vorstrafenregister für jeden Bürger. Allerdings ist die Einsicht natürlich nicht jedem gewährt. Trotzdem muss die Information aber zum Beispiel bei der Aushebung preisgegeben werden, um eine Einteilung in eine spezialisierte Truppengattung zu erhalten. Die Daten sind also vorhanden und werden gebraucht. Das Problem ist vor allem die Sicherheit, dass die Daten nicht ohne Einverständnis von Dritten eingesehen werden. Doch gerade heutzutage können durch kleine Unaufmerksamkeiten plötzlich Daten zum Vorschein

kommen. Ein gutes Beispiel dafür die „geheime“ Faxnachricht an die USA, welche vom Schweizer Militär aus versehen abgefangen wurde. Auch durch Sozial Engineering können Beamte beeinflusst werden, Informationen teils mit teils ohne ihres Wissens preiszugeben.

Eine ähnliche Situation findet man auch bei den Spitälern und den Doktoren. Zumindest bei den grösseren Spitälern sind die Krankendaten digital erfasst und auf Knopfdruck kann man in Erfahrung bringen, welche Blutgruppe man hat, auf was man allergisch ist, welche Krankheiten vorhanden sind usw. Natürlich ist es im Interesse des Klienten, diese Informationen dem Doktor zur Verfügung zu stellen, um nicht jedes mal neu gefragt zu werden, sofern man nach einem Unfall überhaupt noch kommunizieren kann.

4.3 Daten im Internet

Ein bisschen anders sieht das mit den Daten im Internet aus. Nur schon für ein Emailkonto bei GMX sollten sie alle 3 Monate mehrere Seiten Informationen preisgeben über ihre Hobbies, Interessen, Familiensituation und alle möglichen privaten Details. Natürlich kann man diese Umfragen auch umgehen, oder bewusst falsche Information angeben, trotzdem werden diese Informationen meist wahrheitsgetreu ausgefüllt und der Email-Anbieter weiss mehr über sie als ein Bekannter. Die Informationen werden dann meistens so benutzt um Ihnen dann möglichst die Werbung zuzusenden, auf die sie eingehen werden. Doch der Email-Anbieter ist bei weitem nicht der einzige. Bei Amazon.com und Ebay werden alle Einkäufe registriert und es wird ihnen sofort angezeigt, welche Produkte Leute gekauft haben, die dasselbe Buch wie Sie gekauft haben. Sie erhalten personalisierte Angebote, denen sie fast nicht widersprechen können und so wird mithilfe Ihrer Information ihre ganze Zahlungsbereitschaft ausgekostet. Natürlich hat das auch Vorteile, denn sehr wahrscheinlich bekommen sie nirgends genau diese Produkte zu diesem Preis. Dennoch hätten sie sich die Produkte wahrscheinlich nicht geleistet, wenn Sie diese in einem herkömmlichen Laden einzeln gesehen hätten.

Auch ohne Ebay und Amazon gibt es tausende von Seiten wo man zur Mitgliedschaft einige Informationen Preisgeben muss, man freiwillig Informationen ins Netz stellt und früher oder später die Übersicht verliert, wer was woher über wen weiss. So wird es auch immer einfacher, mit einer simplen Internetrecherche einige Hintergrundinformationen über eine beliebige Person zu erhalten wenn man nur deren Namen kennt.

4.4 Eine Frage der Übersicht?

All diese Informationen hat man mal jemandem mitgeteilt, wurden irgendwo publiziert oder sind bewusst oder unbewusst aufgenommen worden. Die meisten Informationen sind unproblematisch und können auch ohne weiteres von der Öffentlichkeit eingesehen werden. Nichtsdestotrotz gibt es mit den modernen Data-Warehouses und den Data-Mining Methoden Möglichkeiten, aus diesen Informationen Korrelationen herauszufinden und Schlüsse zu ziehen die bisher schlicht nicht möglich waren.

Das Problem ist meistens, dass man die Übersicht verliert und plötzlich von etwas heimgesucht wird, was man mal vor 10 Jahren irgendwo angegeben hat oder plötzlich ein altes Foto gefunden wird, welches zu einiger Aufruhr führen kann.

4.5 Kann man Programmen vertrauen?

Allerdings gibt es auch immer einige Informationen, welche man nur an bestimmte Personen weitergeben möchte. Diesen Personen muss man vertrauen können. Im Bezug auf digitale Daten muss man nun nicht mehr einer Person vertrauen, sondern auch noch dem Programm, damit man sichergehen kann, dass keine unberechtigte Person zugriff auf die Daten erhält. Dazu gibt es bei den heutigen Datenbanksystemen zwei hauptsächliche Verfahren der Zugriffsüberwachung:

Es gibt die DAC, discretionary access control (Zugriffskontrolle nach Ermessen) und die MAC, mandatory access control (obligatorische Zugriffskontrolle). Für beide Verfahren

braucht es zuerst eine Festlegung der Zugriffsrechte in der realen Welt, dann eine Autorisierungsmethode für die Zugriffsberechtigten. Die Einhaltung der Zugriffsrechte muss überwacht werden und die Unumgehbarkeit der Schutzmechanismen des Datenbankmanagementsystems muss gewährleistet sein.

Bei der **DAC** werden die Rechte an den einzelnen Objekten den jeweiligen berechtigten Benutzern zugeordnet. Beim positiven Schutzsystem werden alle Zugriffe verboten, ausser die explizit erlaubten, beim negativen Schutzsystem werden einige Zugriffe explizit verboten. Die Verteilung der Rechte kann entweder zentral (einer verteilt alle Rechte) oder dezentral (jeder kann seine Rechte einem weiteren zur Verfügung stellen) geschehen.

Bei der **MAC** werden die Benutzer wie auch die Objekte in Sicherheitsklassen eingeteilt wobei ein Benutzer nur tiefer oder gleich klassierte Informationen lesen kann und nur gleich oder höher klassierte Information schreiben kann.

4.6 Privatsphäre in Zukunft

Gerade im Gebiet des Context-Aware Computings wird der Eingriff in die Privatsphäre immer mehr eine Rolle spielen. Wenn wir bei unseren alltäglichen Handlungen unterstützt werden wollen, werden wir nicht vermeiden können, gewisse Informationen über uns preiszugeben. Sei dies durch Messungen von einem Smart-Shirt oder durch Injektion eines RFID Chips unter die Haut mit Identifikationsmerkmalen, wodurch wir eventuell in Zukunft ID, GA, Pass und Kreditkarte ersetzen könnten.

Es wird immer gewisse Vorteile und gewisse Nachteile geben und wir müssen schlussendlich selbst entscheiden, welche Einbusse in der Privatsphäre wir imstande sind einzugehen, um im Gegenzug andere Vorteile geniessen zu können.

5 Werkzeuge zum Schutz der Privatsphäre

5.1 Proxy Server

Proxy-Server bieten einen sehr einfachen Schutz beim Surfen im WWW. Durch das Benützen eines Proxys werden HTTP-Anfragen über einen Server (Proxy) umgeleitet. Der Proxy führt die Anfrage stellvertretend für den Benutzer aus und sendet danach die erhaltene Nachricht des Zielservers zurück an den Benutzer.

Vorteile:

- Die eigene IP-Adresse wird nicht preisgegeben
- Provider und somit Herkunftsland verschleiert
- Der Zielserver erhält keine Informationen über den verwendeten Browser, Betriebssystem oder die verwendete Sprache. Dies kann teilweise auch ein Nachteil sein.

Nachteile:

- Identifikation durch gesetzte Cookies noch immer möglich
- User muss dem Proxy vertrauen
- typischerweise Geschwindigkeitseinbussen
- Offene, anonyme Proxies sind selten

Beispiele:

- proxy.unizh.ch
- www.anonymizer.com

5.2 Proxy Ketten

Beim Benutzen eines einzelnen Proxys besteht die Gefahr, dass genau dieser Proxy-Server ausspioniert wird oder selber Daten über die Benutzer sammelt. Der Benutzer muss dem Proxy-Server vertrauen. Dieses Vertrauensproblem kann durch so genannte Proxy-Ketten (Proxy Chains) entschärft werden. Hierbei werden die Anfragen der Benutzer über mehrere, möglichst unabhängige Proxies weitergeleitet. Optional werden die Anfragen mittels

asynchronem Verfahren verschlüsselt, sodass auch kompromittierte Zwischenstationen die Kommunikation nicht mitlesen können.

Vorteile:

- Entschärfung des Vertrauensproblems
- Sehr unwahrscheinliche Rückverfolgung

Nachteile:

- weitere Geschwindigkeitseinbussen
- Probleme mit Cookies bleiben bestehen

Beispiele:

- JAP[11]

5.3 Remailer

E-Mails enthalten mehr Informationen, als vielen Benutzern bekannt ist. Neben der IP des Absenders sind oft auch Rechnername und benutzter Mailclient aus dem Header ersichtlich. Microsoft Outlook verrät hier sogar, in welcher installierten Version es vorliegt. Remailer sind Server, die den gesamten Header einer E-Mail löschen und die Mail danach mit einem leeren oder vom Benutzer frei bestimmten Header an den Empfänger zustellen. Auch hier lässt sich das Vertrauensproblem durch eine Kette von Remailern und zusätzlicher asynchroner Verschlüsselung lösen. Sehr unbeliebt sind die verräterischen Header auch in Newsgroups (Usenet), da die Nachrichten möglicherweise von vielen tausenden von Menschen gelesen werden. Mit der Methode der Remailer lassen sich E-Mails und Posts in Newsgroups anonymisiert zustellen.

Vorteile:

- Remailer ermöglichen den Versand anonymer E-Mails und Posts in Newsgroups

Nachteile:

- Missbrauch durch Spammer
- Service ist vergleichsweise unzuverlässig (relativ hohe Quote von nicht zugestellten E-Mails)

- Zustellung kann mehrere Stunden dauern

Beispiele:

- Windows: Quicksilver[12]
- Unix, Windows und Mac: Mixmaster[13]

```
Received: from exsmtp01.agrinet.ch ([10.50.250.200]) by
EXVS01.mcis.agrinet.local with Microsoft SMTPSVC(6.0.3790.211);
      Wed, 14 Jun 2006 18:42:24 +0200
Received: from mail.messaging.ch ([10.50.250.212]) by
exsmtp01.agrinet.ch with Microsoft SMTPSVC(6.0.3790.211);
      Wed, 14 Jun 2006 18:42:24 +0200
Received: from mail.gmx.net ([213.165.64.21])
     by mail.messaging.ch with
     id lUil1U00D0TWjyD0000000
     for mark@freihof-schmidrueti.ch; Wed, 14 Jun 2006 18:42:46
+0200
X-IMP: RBL SBL+XBL: 0.00,RBL SPAMCOP: 0.00,RBL SORBS: 0.00,RBL
MAPS_ORDB: 0.00,URL RHS: 0.00,URL SURBL: 0.00
Received: (qmail invoked by alias); 14 Jun 2006 16:42:20 -0000
Received: from pub212004083069.dh-hfc.datazug.ch (EHLO Dellalex)
[212.4.83.69]
  by mail.gmx.net (mp030) with SMTP; 14 Jun 2006 18:42:20 +0200
X-Authenticated: #1985444
From: "Alexander" <alexanderbucher@gmx.ch>
To: "'Mark Furrer'" <mark@freihof-schmidrueti.ch>
Subject: AW: PS
Date: Wed, 14 Jun 2006 18:42:25 +0200
Message-ID: <000201c68fd1$84beee40$6500a8c0@Dellalex>
MIME-Version: 1.0
Content-Type: multipart/mixed;
     boundary="----=_NextPart_000_0003_01C68FE2.4847BE40"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.2616
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2869
Importance: Normal
In-Reply-To: <EXSMTP01koTvYkkvpTy0005b419@exsmtp01.agrinet.ch>
X-Y-GMX-Trusted: 0
Return-Path: alexanderbucher@gmx.ch
X-OriginalArrivalTime: 14 Jun 2006 16:42:24.0373 (UTC)
FILETIME=[837F4250:01C68FD1]
```

Der E-Mail Header enthält neben der IP des Absenders auch den Rechnernamen sowie oft auch Informationen über den Mail-Client.

5.4 Das anonyme Netzwerk TOR

Tor ist ein sehr vielseitig einsetzbares Programm. Es setzt direkt auf der TCP-Schnittstelle auf und bietet somit grundsätzlich ein anonymes Netzwerk für alle auf TCP basierenden Dienste. Das Ketten-Prinzip inklusive Verschlüsselung ist dabei nicht neu, sondern wird einfach für sämtliche Dienste und Ports erweitert. Die Spezialität des Tor-Netzwerkes ist seine Dynamik. Jeder Tor-Benutzer wird dazu aufgefordert, auf seiner Maschine ebenfalls einen Tor-Server zu installieren. Dadurch wird ein breites dynamisches Netzwerk geschaffen, durch das TCP-Verbindungen verschlüsselt weitergeleitet werden. Die Länge der Kette kann der Benutzer dabei frei bestimmen.

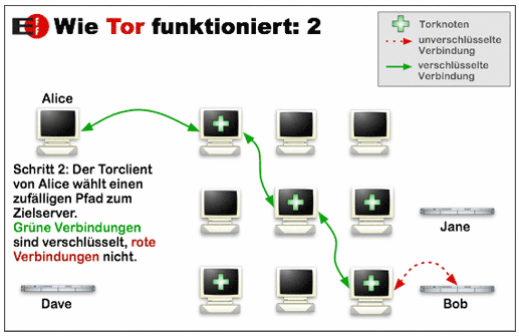

Abb. 1: Funktionsweise von Tor
Quelle: http://tor.eff.org/overview.html.en

Vorteile:

- Basis für sämtliche auf TCP basierende Dienste
- Anonymisierung durch Chain-Forwarding und Verschlüsselung

Nachteile:

- Gefahr des Missbrauches für illegale Zwecke
- Viele langsame Server, die den Verkehr ausbremsen

Projekt Homepage:

- http://tor.eff.org/index.html.en

6 Quellenangaben

[1] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harvard Law Review 193-220 (1890)

[2] Robert Ellis Smith, Ben Franklin's Web Site 6 (Sheridan Books 2000)

[3] Pressemitteilung des U.S. Department of Homeland Security: „Fact Sheet: US-Visit“: http://www.dhs.gov/dhspublic/display?content=4047 (27.09.2004)

[4] Pressemitteilung der Bundesbehörde der Schweizerischen Eidgenossenschaft: „Kampf gegen Rassismus, Hooliganismus und Gewaltpropaganda verstärken“: http://www.admin.ch/cp/d/3e4a22db_1@presse1.admin.ch.html (12.02.2003)

[5] Entwurf des „Bundesgesetz über Massnahmen gegen Rassismus, Hooliganismus und Gewaltpropaganda“, siehe http://www.fedpol.admin.ch/fedpol/de/home/dokumentation/medieninformationen/2003/ref_2003-02-120.html

[6] Mitteilung des Eidgenössischen Datenschutzbeauftragten in Sachen Hooliganismusbekämpfung: http://www.edsb.ch/d/doku/pressemitteilungen/2006/2006-06-09.htm (09.06.2006)

[7] Bundesamt für Sozialversicherung: „Die Versichertennummer“: http://www.ahv.ch/Home-D/allgemeines/31810612d.pdf (gültig ab 1. Januar 1994)

[8] International Conference of Data Protection & Privacy Commissioners "Resolution on Radio-frequency Identification," Final Version, November 20, 2003, siehe: http://www.privacyconference2003.org/resolutions/res5.doc

[9] Spy Satellites: The Next Leap Forward," International Defense Review, January 1, 1997

[10] Google Earth, erreichbar über http://earth.google.com/

[11] JAP Homepage: http://anon.inf.tu-dresden.de/

[12] Quicksilver Homepage: http://kai.iks-jena.de/quick/quicksilver1.html

[13] Mixmaster Homepage: http://mixmaster.sourceforge.net/