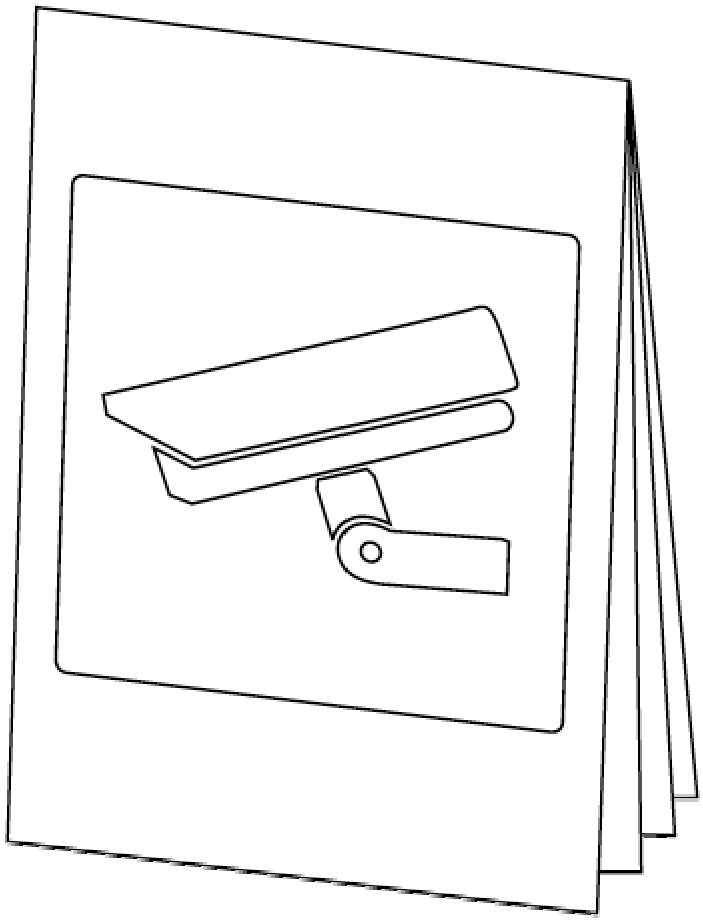
# Wie beeinflusst die heutige
# ÜBERWACHUNG
## unsere Lebensqualität?



**Andreas Ruckstuhl**
andy@open-minded.ch

**IS2002c**
**Fr. Amrei Gerhards**

Abgabetermin: **07.07.2005**

# INHALTSVERZEICHNIS

# EINLEITUNG

## Themenwahl

Die Findung dieses Themas war für mich keine grosse Sache, weil es mich sehr interessiert und auch fasziniert. Ein weiterer und wichtiger Punkt für die Themenwahl war die Aufklärung, da die meisten Personen sich nicht bewusst sind, inwieweit sie im alltäglichen Leben von privaten Firmen und öffentlichen Behörden überwacht werden.

Ich habe deshalb vor, diese Arbeit nach Abschluss auf meiner Website www.open-minded.ch (welche sich auch mit dem Thema Überwachung beschäftigt) zu veröffentlichen.

Das Leitthema „Lebensqualität" bezieht sich hier auf das subjektive Befinden jeder Person. Manche interessiert es nicht, dass sie überwacht werden, andere finden es interessant und wieder andere stören sich daran und sehen in der Überwachung eine Verminderung ihrer Lebensqualität.

## Persönlicher Zugang

Da ich mich bereits seit einiger Zeit für dieses Thema interessiere, habe ich auch schon einige Informationen dazu gesammelt.

Meine Meinung zum Thema Überwachung hat sich immer kritischer entwickelt, je mehr ich erfahren konnte, insbesondere durch die SF-Spezial Sendung von SF DRS, welche sich eine Woche lang intensiv mit dem Thema Überwachung und dem „gläsernen" Menschen beschäftigt hat.

Kritisch heisst in diesem Fall fast empört. Dass wir „auf Vorrat" überwacht werden (insbesondere über unser Mobiltelefon, welches ständig unsere Position übermittelt) fand ich dann doch etwas übertrieben, ebenfalls fühlte ich mich in meiner Privatsphäre gestört. Wenn ich irgendwo hin gehen will, ohne dass mich jemand dahin zurückverfolgen kann, darf ich keine Kreditkarten, kein Mobiltelefon verwenden. Und überhaupt mit niemandem sprechen; interagieren allgemein.

Deshalb kommen wir wieder auf die eigentliche Fragestellung zurück: *Wie beeinflusst die heutige Überwachung unsere Lebensqualität*?

## Zielformulierung

Folgende Ziele möchte ich in dieser Arbeit erreichen:

- Ich möchte den Umfang der heutigen Überwachung untersuchen.
  - Wer überwacht uns?
  - Welche Lebens- und Alltagsbereiche werden überwacht?
  - Welche Daten wurden über mich gesammelt?
- Ich möchte feststellen, inwieweit Überwachung unsere Lebensqualität erhöht oder vermindert.
  - Welchen Nutzen ergibt sich für den/die Überwachten?
  - Welche Methoden werden angewendet?
- Ich möchte anhand einer Umfrage feststellen, wie die Bevölkerung zur verminderten Privatsphäre steht und ob Ängste bezüglich des „gläsernen" Menschen bestehen.
- Des Weiteren möchte ich die Finanzierungsarten und die gesetzlichen Grundlagen erfahren.
  - Welche Gesetze erlauben/verbieten gewisse Überwachung?
  - Wie wird die private und die staatliche Überwachung finanziert?

# HAUPTTEIL

## Kleine Umfrage, Meinungen aus Bekanntenkreis

Ich habe auf meiner Homepage www.open-minded.ch eine Umfrage geschaltet, um zu Erfahren, wie stark sich die Öffentlichkeit überwacht fühlt. Hier das Ergebnis:

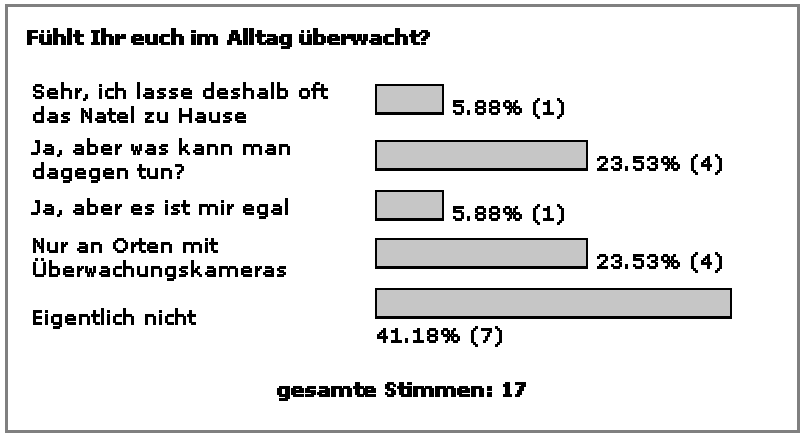



*Abb. 1: Ergebnis der Umfrage auf open-minded.ch*

Diese Umfrage ist nicht repräsentativ und kann möglicherweise nicht der Wirklichkeit entsprechen (gemäss meiner Einschätzung nahmen nur Personen zwischen 16 und 55 Jahren in meinem Bekanntenkreis teil). Der aktuelle Stand der Umfrage kann unter www.open-minded.ch abgerufen werden.

Aufgrund dieses Ergebnisses stellt man fest, dass fast die Hälfte (rund 40%) der Teilnehmer sich nicht an der momentanen Situation bezüglich der Überwachung stört.

Eine weitere Gruppe (rund 25%) fühlet sich nur an Orten mit Überwachungskameras überwacht. Teilnehmer einer weiteren Gruppe (ebenfalls 25%) sind besorgt über die heutige Überwachung, wissen jedoch nicht, was sie dagegen tun können.

Diese Haltungen stellte ich auch bei diversen Diskussionen rund um den Datenschutz und die Überwachung mit Bekannten fest. Viel gehörte Argumente gegen den Datenschutz:

- Warum ist es schlecht, wenn ich nur Werbung zu den für mich interessanten Produkten bekomme?
- Wo ist der Unterschied zwischen der heutigen Werbung und der personifizierten Werbung in der Zukunft bezüglich der Entscheidungsfreiheit?
- Ich habe nichts zu verbergen, somit ist es mir egal, wenn mich jemand überwacht.

Letztere Frage bekommt man sehr oft und als erste Antwort zu hören. Viele dieser Personen reagieren jedoch mehr als nur kritisch auf die Frage „Kann ich mal kurz Deine SMS' lesen?" und antworten mehr oder weniger energisch mit „Was gehen Dich meine SMS' an?".

Dies ist für mich eine paradoxe Haltung. Einem Familienangehörigen oder einem guten Bekannten möchte man seine SMS auf keinen Fall zeigen, dass aber diese SMS alle aufgezeichnet werden und bei Bedarf von jedem (nicht) berechtigten Mitarbeiter (den man nicht kennt) gelesen wird, stört die meisten Personen nicht.

Meiner Meinung nach sollten sich Viele fragen, wem sie vertrauen und wem nicht.

# Eidgenössischer Datenschutzbeauftragter

## Interview

Die Aufgabe des Eidgenössischen Datenschutzbeauftragten ist unter anderem, die Zitat „Beratung von privaten Personen“ (Angabe auf der Website www.edsb.ch). Aufgrund dieser Angabe sandte ich ein E-Mail mit diversen Fragen und einer Interviewanfrage an die angegebene Adresse.

Leider wurden meine Erwartungen nicht im Geringsten erfüllt. Als Antwort bekam ich ein Standartmail, in welcher sich der Eidg. Datenschutzbeauftragte erfreut zeigte:

> Wir begrüssen es sehr, dass an Schulen und Universitäten der Schutz und die Gefährdung der Persönlichkeitsrechte thematisiert und als Gegenstand von Vorträgen, Haus- und Diplomarbeiten gewählt wird.

Leider verfügten sie nicht über das notwenige Personal und Ressourcen, um für mich Unterlagen zusammenzustellen und einen Interviewtermin zu organisieren und durchzuführen.

Deshalb werde ich nachfolgend kurz die Informationen auf der Webseite des EDSB zusammenfassen.

## Tätigkeit

Der Eidgenössische Datenschutzbeauftragte hat folgende zentralen Aufgaben:

- Aufsicht über Bundesorgane
- Aufsicht über Privatpersonen
- Beratung von privaten Personen
- Unterstützung und Beratung der Organe des Bundes und der Kantone
- Stellungnahme zu Rechtsvorlagen des Bundes
- Zusammenarbeit mit in- und ausländischen Datenschutzbehörden
- Information der Öffentlichkeit
- Führung und Veröffentlichung des Registers der Datensammlungen.

Er ist somit der sprichwörtliche staatliche Wächter der Privatsphäre von uns Bürgern.

# Big Brother Awards

## Was ist Big Brother Awards?

Big Brother Awards wurde laut seiner Website ins Leben gerufen, „um die öffentliche Diskussion über Privatsphäre, Überwachung und Datenschutz zu fördern“.

Mit diesem Preis werden die grössten Schnüffelratten der Schweiz aus Privatwirtschaft und Politik ausgezeichnet. Ebenfalls ausgezeichnet werden die so genannten „Winkelriede“, welche sich aktiv für den Datenschutz einsetzen.

Ein Gewinner des Big Brother Awards ist z.B. das VBS (für den Einsatz von unbemannten Überwachungsdrohnen gegen Privatpersonen im Inland und den Fragenbogen bei der neuen Aushebung, bei welcher die Stellungspflichtigen ca. 600 Fragen beantworten müssen, darunter auch solche nach Selbstmordgedanken, Missbräuche, Drogenerfahrungen und sexueller Vorlieben).

Gewinner des gegenteiligen Awards ist z.B. die Medienkünstlerin Annina Rüst, welche mit ihren Projekten auf das Thema Überwachung hinweist sowie Bert Setzer (Pseudonym), welcher die Q-Card erfand, welche als Ersatz für die M-Cumulus und die Coop Supercard funktioniert (man bekommt ebenfalls alle Rabatte), jedoch benutzen dann diverse Leute die selbe Kartennummer und man ist beim Anbieter nicht registriert. So bleibt man anonym, ohne dass man die erwähnten Rabatte nicht beanspruchen könnte.

# Datamining

## Was ist Datamining?

Unter Datamining versteht man das systematische Entdecken und Extrahieren von noch unbekannten Informationen aus grossen Datenmengen. Dies geschieht in der Regel automatisiert über spezielle Datenbankabfragen oder halbautomatisch mit Hilfe von erstellten Statistiken, welche dann durch Experten ausgewertet werden.

Das Ziel ist das Finden von Regeln und Auffälligkeiten in der oben erwähnten Statistik.

In der Forschung mit der künstlichen Intelligenz (KI) wird auch auf das Prinzip des Dataminings gesetzt, es entspricht in vielen Punkten einem neuronalen Netz.

## Weshalb ist Datamining für den Staat und die Wirtschaft interessant?

Durch die oben erwähnten Verfahren lassen sich z.B. Änderungen im Verhalten von Kundengruppen, oder eben von einzelnen Kunden aufspüren und die Geschäftsstrategie kann dann explizit darauf ausgerichtet werden.

Für den Staat ist Datamining vor allem in der Strafverfolgung interessant. Spezialisierte Experten, so genannte Profiler, wenden das Prinzip des Dataminings auf bekannte Informationen des gesuchten Täters an, um seine weitere Vorgehensweise voraussagen zu können.

## Bevormundung und Manipulation als Folge der Datenhaltung

Jeder kennt das Sprichwort „Wissen ist Macht“, welches im kalten Krieg durch den KGB und die CIA mehr als nur ernst genommen wurde.

Heute passt das Sprichwort eher zu neuen Marketinginstrumenten, insbesondere dem Datamining, dessen Datenbasis z.B. bei Migros durch Kundenkarten generiert wird. Im Internet stellt der Buchhandelsriese Amazon wohl das prominenteste Beispiel für Datamining dar.

Ich möchte hier mit einem Text aus einer Arbeit von der Universität Zürich anhand des Beispiels Amazon aufzeigen, wie eine Bevormundung und Manipulation genau aussieht oder aussehen könnte:

> Ja, dieser attraktive Bücherladen, der ständig offen hat und wohl jedes Buch anbietet. Dazu liefert Amazon möglichst noch Rezensionen und weitere Bücher, ganz nach unserem Geschmack, die einem zum günstigen Set-Preis angeboten werden. Beim nächsten Besuch werden wir nicht nur persönlich begrüsst, nein es wird uns für die Bestellung gedankt und wir können gleich noch nachschauen, welchen Status unsere Bestellung hat.
>
> Doch soweit soll es gar nicht kommen, denn plötzlich entdecken wir unten ein sehr spannend erscheinendes Buch – oder nein, es ist eine DVD. Eigentlich ganz praktisch, jetzt wo gerade unser DVD Player (natürlich auch über Amazon bestellt) angekommen ist.
>
> Und so geht unsere Shoppingtour weiter. Wir werden immer wieder mit netten persönlichen Angeboten, Reduktionen oder gar Fragen überrascht, welche uns das attraktive Angebot von Amazon näher bringt. Mit diesen Fragen lässt sich sogar Geld verdienen, hei das macht Spass! Alles sieht auf den ersten Blick ganz toll und nett aus. Wir bauen ein richtig warmes Verhältnis zu diesem online Buchladen auf, der unseren Geschmack immer wieder trifft, die Welt scheint einfach nur gute Bücher zu produzieren.
>
> Bis endlich die Frage in uns auftaucht – ja woher weiss denn der alles? Die haben mich nie nach meinem Geschmack gefragt. Was wissen die denn noch über mich?

**Bevormundung**
Eine Bevormundung tritt dann ein, wenn man ein Produkt sucht, welches das benutzte System nicht zur „normalen“ Produktgruppe des Benutzers zählt. Erst nach (evtl. umständlichen) Suchen findet man das gewünschte Produkt.

Während der Suche wird man immer wieder mit der „normalen“ Produktgruppe und dessen Spezialangeboten konfrontiert.

Somit ist man von der normalen Entscheidungsfreiheit bei einer „offline“ Buchhandlung weit entfernt, welche dem Kunden immer alle verfügbaren Bücher zeigt.

**Manipulation**
Die Gefahr durch Manipulation der Kunden wird erst in Zukunft zu einem wichtigen Thema werden. Je mehr Informationen zu einem Kunden zur Verfügung stehen, je besser kennt der „Datensammler“ die Wünsche und Interessen der jeweiligen Person.

Es gibt bereits heute Technologien, die unserem Hirn Geschmackseindrücke via Ultraschall vermitteln können. Man weiss auch, dass verschiedene Geschmäcker unterschiedliche Gefühle hervorrufen. Wer sich gut fühlt, der kauft mehr.

In Zukunft wird man die Abläufe in unserem Gehirn weit besser kennen als heute, die technischen Mittel zur Manipulation des selben werden ebenfalls fortschrittlicher sein. Alles nur eine Frage der Zeit. Und dies ist nur ein kleiner Ausschnitt aus den verschiedenen Möglichkeiten!

Wer diese Zukunft nicht wünscht, kann entweder politisch aktiv werden, um den Datenschutz zu verbessern, oder man verzichtet auf Kundenkarten und kauft in Zukunft zielgerichteter ein.

# Überwachung durch RFID

## Was ist RFID?

RFID steht für **R**adio **F**requency **Id**entification (Funk-Erkennung) und ist eine Methode, um Daten berührungslos und ohne Sichtkontakt lesen und speichern zu können.

Diese Technologie soll in erster Linie die EAN Strichcodes (welche wir von jedem Produkt aus dem Supermarkt kennen) ersetzen und die Abwicklung des Bezahlvorgangs beschleunigen (es müssen nicht mehr alle Produkte über den Scanner gezogen werden, die Auslesung der Daten erfolgt berührungslos).

## Welche Vorteile hat RFID?

Die Hersteller und Befürworter von RFID sehen die Vorteile vor allem in folgenden Bereichen:

- Identifikation von Banknoten
- Tieridentifikation
- Patientenidentifikation
- Waren- und Bestandsmanagement
- Zutrittssysteme
- Positionsidentifikation

Der Vorteil der Technologie im Allgemeinen ist das berührungslose Auslesen oder Speichern der Daten.

## Welches sind die Gefahren dieser Technologie aus Datenschutzgründen?

**Zusätzliche, nicht dokumentierte Speicherzellen**
Es ist durchaus denkbar, dass weitere Speicherzellen eingebaut werden, auf die nur mit speziellen Kommandosequenz zugegriffen werden kann. Welche Informationen werden darin gespeichert?

**Verlust der informationellen Selbstbestimmung**
Die einzelne Person hat mit RFID Sendern keinen Einfluss mehr darauf, wer auf die Daten zugreift, welche man mit sich herumträgt. Ebenso können auch nicht berechtigte Personen auf die Daten Zugriff nehmen (besonders in den ersten paar Jahren der Einführung; bei WLAN ging es nicht lange bis die Verschlüsselung WEP geknackt wurde).

Falls wir in Zukunft für die Krankheitsgeschichte einen Chip implantiert bekommen werden (in den USA gibt es bereits Firmen, welche solche Geräte und Implantierungen anbieten), kann der Arzt in einem Notfall sofort die Blutgruppe und Allergien erfahren.

Leider kann auch ein möglicher Arbeitgeber (zwar unrechtmässig, aber wer überprüft das?) bereits Ihre Krankheitsgeschichte auslesen und feststellen, ob sie in Zukunft oft krank werden oder nicht und Sie auch aufgrund dessen einstellen oder eben nicht.

Soviel zur ärztlichen Schweigepflicht...

## Telekommunikationsüberwachung durch den Staat

### Satos 3, Onyx

*Abb. 2: Onyx Bodenstation Leuk (VS)*

Onyx ist das schweizerische System für die Kommunikationsüberwachung. Über die drei Stationen in Leuk (siehe links, Abb. 2), Heimenschwand und Zimmerwald (wo ein Supercomputer in einem Bunker die gewonnenen Informationen auswertet) werden diverse Telefongespräche, Fax- und E-Mailnachrichten abgehört. Rund vierzig Mitarbeiter des VBS werten dort die gewonnenen Daten nach Stichworten aus.

Nach Angaben von Paul Günter, SP-Nationalrat und Mitglied der Sicherheitspolitischen Kommission, wird zurzeit nach 5000 definierten Schlüsselwörtern gesucht. Von den ausgewerteten Daten profitiert in erster Linie der Strategische Nachrichtendienst.

Onyx lief seit April 2000 im Probebetrieb und ist seit Mitte 2004 im operationellen Betrieb, welcher Ende 2005, Anfang 2006 vollständig erreicht werden soll. Bis dann müssen die Zahl der Antennenstandorte verdoppelt werden.

Den Entscheid für Onyx wurde vom Bundesrat am 13. August 1997 auf Vorschlag des VBS getroffen.

#### Finanzierung

Der genaue Grad der Finanzierung ist immer noch unbekannt. Diverse Anfragen aus dem National- und Ständerat an das VBS wurden nur ausweichend beantwortet. Die Erstellung eines solchen Systems (das von aus Satos-3 ausgeht, welches den Kurzstreckenfunk überwachte) wurde ebenfalls vor dem National- und Ständerat verheimlicht. Erst eine undichte Stelle (ein Gemeinderat von Heimenschwand) äusserte sich am Stammtisch zu Onyx, diese Informationen gelangten zu einem Reporter der Zeitung „Der Bund“, welcher dann das Thema aufnahm und an die Öffentlichkeit brachte. Man rechnet jedoch mit einem Gesamtbetrag von rund 100 Millionen SFr..

#### Gesetzliche Grundlagen

Der Strategische Nachrichtendienst SND (welcher Onyx betreibt) ist dem Militärgesetz unterstellt, welches unter anderem die Nachrichtenbeschaffung im Ausland regelt.

Onyx ist demnach an folgende Richtlinien gebunden:

- Onyx darf nur für Abhörungen ausserhalb der Landesgrenzen verwendet werden.
- Onyx darf nicht für die konventionelle Strafverfolgung verwendet werden.
- Die Weitergabe von erhaltener Informationen an den Inlandgeheimdienst ist strikte geregelt: Es dürfen keine Überwachungen „auf Vorrat“ gemacht werden.

### Zweck dieser Überwachung

Es gibt verschiedene Gründe, warum die Schweiz ein solches Überwachungssystem besitzt:

- Militärische Zwecke (in der Schweiz eher untergeordnet)
- Verhinderung der Verbreitung von Massenvernichtungswaffen
- Terrorismusbekämpfung
- Kontrolle der Einhaltung von Embargos
- Verbrechensbekämpfung
- Industriespionage

Die aus diesen Zielen heraus gewonnenen Daten werden dann auch mit anderen Geheimdiensten getauscht:

## Austausch der Informationen unter Geheimdiensten

Der Austausch von gesammelten Informationen mit anderen Geheimdiensten verläuft laut dem Chef des Strategischen Nachrichtendienstes, Hans Wegmüller, (in seinem einzigen Interview mit dem Schweizer Fernsehen) folgendermassen. Es werden z.B. keine Rohdaten sondern nur ausgewertete Informationen weitergegeben. Als „Bezahlung“ dafür erhalten unsere Schweizer Nachrichtendienste ebenfalls ausgewertete Informationen.

Weitere (und vor allem genauere) Informationen waren leider aufgrund der hohen Geheimhaltungsstufe nicht zu erfahren.

## Echelon

### Wieso dieses Kapitel?

Grundsätzlich möchte ich mich eigentlich nur mit Themen beschäftigen, welche in der Schweiz wichtig und gegenwärtig sind. Echelon ist ein amerikanisches Überwachungssystem, welches diverse Kommunikationssatelliten und internationale Telefongespräche und Fax- und E-Mailnachrichten überwacht. Da dieses System jedoch auch Gespräche und Nachrichten von und in die Schweiz erfasst, möchte ich Echelon deswegen mit einbeziehen. Weiter wird dem Schweizer Onyx System (siehe oben) eine gewisse „Mittäterschaft“ zugetraut, da die Swisscom die am Onyxstandort in Leuk (VS) installierte Anlage an eine amerikanische Telekommunikationsfirma („Veristar“, Betreiber „Americom“) verkauft hat, welche intensiv mit der NSA zusammen arbeitet.

Der Bericht der GPDel vom 10. November 2003 über das Projekt Onyx hält jedoch fest, dass bis zum damaligen Zeitpunkt keine Zusammenarbeit vorhanden ist.

### Funktion

Echelon ist ein Überwachungs- und Abhörsystem, welches von den USA, England, Kanada, Australien und Neuseeland betrieben wird. Für das Auswerten der gesammelten Daten werden die leistungsfähigsten Computer eingesetzt. Diese Computer, Dictionarys genannt, sind über die USA, England und Australien miteinander verbunden.

Wenn nun jemand in einem abgehörten Gespräch den Namen, die Kontonummer einer gesuchten Person oder andere vorher definierte Wörter verwendet, erkennt dies der Computer und gibt diese Informationen dann zur weiteren Auswertung an die NSA Hauptzentrale. Laut der SF-Spezial Sendung werden dort die gewonnenen Daten dann von 38'000 Angestellten ausgewertet. Es ist auch zu sagen, dass die USA nie abgestritten haben, mit Echelon Industriespionage zu Gunsten von US-Unternehmen durchzuführen.

Zum Vergleich: Die NSA verfügt laut dem Bericht der Schweizerischen Geschäftsprüfungsdelegation zum Thema Onyx über ein Budget von über 3,6 Mia. US-Dollar, das ist grösser als dasjenige von CIA und FBI zusammen.

## Fichenaffäre

Ich möchte an dieser Stelle die Fichenaffäre nur kurz anschneiden, um eine kurze Übersicht zu geben.

Während des Kalten Krieges liessen Bundespolizei und Bundesanwaltschaft nicht nur Handlungen mutmasslicher Staatsschutzkriminalität, sondern bis 1989 auch rund 900'000 Personen und Organisationen aus dem linken Umfeld präventiv beobachten, obwohl für diese Massnahmen keine rechtlichen Grundlagen bestanden.

Es war vorgesehen, dass etwa 10'000 als politisch gefährlich eingestufte Bürgerinnen und Bürger im Krisen- oder Kriegsfall inhaftiert hätten werden sollen. Mit der Fichierung sollte angeblich erreicht werden, dass die Schweiz vor kommunistischen "Subversiven" geschützt werde. Die Aufdeckung des Fichenskandals durch Feststellungen der parlamentarischen Untersuchungskommission PUK-EJPD, die vom heutigen Bundesrat Moritz Leuenberger präsidiert wurde, führte zu einem weit reichenden Aufschrei. Das Vertrauen in den Staat war erschüttert.

Als Konsequenz dieser Affäre musste die damalige Bundesrätin und EJPD Vorsteherin Elisabeth Kopp auf Druck der Öffentlichkeit zurücktreten.

Die Fichenaffäre wird in der Schweiz immer wieder gern zitiert, wenn es um Datenschutz und dessen Anwendung geht.

# Überwachung durch Mobilfunkbetreiber

## Standortbestimmung

Der Mobilfunkbetreiber weiss immer genau, wo sich ein eingeschaltetes Mobiltelefon befindet. Diese Daten kann und muss er aufzeichnen.

Es gibt zwei verschiedene (technische) Möglichkeiten, wie er an diese Daten kommt.

### Eingebuchte Zelle

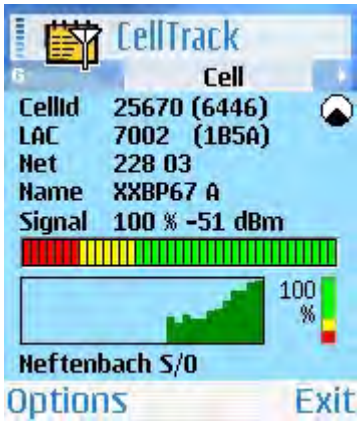



*Abb. 3: CellTrack (6600)*

Unsere Mobiltelefone verwenden alle den GSM Standart (900MHz und 1800MHz, Dualband). Darin wird definiert, wie sich die Mobiltelefone bei den Antennen anmelden. Jede Antenne ist in sich eine Zelle (die aktuelle kann man auf verschiedenen Handytypen mit spezieller Software wie CellTrack anzeigen lassen; siehe Abb. 1). Diese Zellen sind je nach Bevölkerungsdichte unterschiedlich gross.

Jedes Handy bucht sich bei der Zelle mit der besten Empfangsqualität ein. Dies kann auch während eines Gesprächs ohne Unterbruch passieren (dieser Vorgang nennt man Handover).

Während einer Testfahrt mit dem Intercity von Winterthur nach Zürich wechselte mein Natel 31 mal die Funkzelle.

Der Mobilfunkbetreiber weiss (durch eine Datenbankabfrage) somit immer, in welcher Zelle sich das gesuchte Mobiltelefon befindet.

### Dopplerpeilung

Diese Peilung funktioniert sehr genau, jedoch nur, wenn das Mobiltelefon Funkkontakt zu mindestens drei Antennen hat. Es wird immer nacheinander eine Antenne an den Empfänger geschaltet, so dass sich eine "elektronische Rotation" der Empfangsantenne ergibt, ca. 300 Umdrehungen in der Sekunde. Bewegt sich das Mobiltelefon dem Funksignal entgegen, so erhöht sich geringfügig die Empfangsfrequenz, entfernt es sich, so wird die Frequenz des Empfangssignals minimal niedriger. Somit kann man die Position exakt bestimmen, da man die genaue Position der Antennen kennt.

## Aufzeichnung aller Gespräche und SMS

In der Schweiz sind alle Telefon- und Mobilnetzbetreiber verpflichtet, den Ort des Gesprächs, die Dauer, der Gesprächspartner und das Gespräch selber mindestens 6 Monate aufzubewahren. Dies bestätigt auch Monika Walser, Pressesprecherin der Sunrise gegenüber dem Schweizer Fernsehen in einem Interview Ende November 2004:

> Wir sind verpflichtet, diese Daten während 6 Monaten zu speichern, und zwar das Gespräch und wo das Gespräch stattgefunden hat. Wir dürfen diese Angaben nur herausgeben, wenn dies durch eine behördliche Strafuntersuchung angeordnet wird. Dies kommt ca. ein bis zwei Mal pro Monat vor.

## Ergebnis der Anfrage

Ich versandte auch meinem Mobilfunkprovider (Orange) ein Auskunftsbegehren über die über mich gesammelten Daten.

Nachdem mich die Orangemitarbeiterin freundlich per Telefon aufgefordert hatte, eine Kopie meiner ID nach Lausanne zum Orange Hauptsitz zu senden, kam am 8. Juni 05 ein eingeschriebener Brief, in welchem man mir mitteilte, dass folgende Daten von mir bei Orange gespeichert sind:

- Meine Personalien (Name, Adresse, Nationalität, Geburtsdatum)
- Rechnungsdaten (Art und Intervall der Bezahlungen, ausstehender Betrag)
- Aboinformationen (Nummer, MNP Migrationstatus, Aktivierungsdatum, Typ der Ausweiskopie (ID, Pass, Fahrausweis), Korrespondenzsprache)

Es wurden mir leider keine Ortsangaben (wie oben beschrieben) gemacht.

# Überwachung durch Internetprovider

## Zugewiesene IP-Adressen

Aufgrund der Auskunftspflicht der Internetprovider (BÜPF Art. 14.4) müssen sie die jeweils per DHCP zugewiesenen IP Adressen der Kunden protokollieren und mit dem jeweiligen Abonnementen in Verbindung bringen.

> Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen.

Die Protokollierung der Besuche auf den jeweiligen Servern ist Sache des Serverbetreibers.

## Ergebnis der Anfrage

Ich sandte eine Anfrage bezüglich der über mich gespeicherten Daten an Cablecom. Diese meinte jedoch folgendes:

> Leider haben wir keine Kundendaten von Ihnen (...).
> Möglicherweise sind Sie umgezogen (...)

Da ich jedoch nicht umgezogen war, sandte ich Cablecom in Referenz auf dieses Schreiben alle Daten, welche mir vorlagen, um eine schnelle Abwicklung zu gewährleisten.

Ca. 1 Woche später rief mich eine Mitarbeiterin der Cablecom an, und fragte mich ganz erstaunt, um was es gehe. Seit ich ihr den Sachverhalt noch einmal explizit erklärte hörte ich nie wieder etwas von der Cablecom (ausser natürlich die monatliche Rechnung).

Somit kann ich also keine speziellen Angaben zur Datensammelpraxis bei der Cablecom GmbH machen.

Den Allgemeinen Geschäftsbedingungen unter Punkt 12 kann man jedoch folgendes zum Datenschutz entnehmen:

> Der Kunde stimmt zu, dass cablecom im Zusammenhang mit der Erbringung der Dienstleistungen, insbesondere zwecks Leistungsverbesserung, Abwicklung der Kundenbeziehung oder zu Inkassozwecken, Kundendaten an ausgewählte Dritte weitergeben kann.
>
> cablecom darf Kundendaten auch zu Marketingzwecken für sich und ausgewählte Partnerfirmen verwenden, soweit der Kunde die Verwendung nicht ausdrücklich untersagt hat.

Diese Klausel umfasst nur die Nutzung der Personendaten (Name, Adresse, etc.) und schliesst Datamining nicht mit ein.

# Zusammenfassung Mobiltelefon- und Internetprovider

Die Kundenüberwachung durch die ISPs und Mobiltelefonanbieter ist also minim und geht nur so weit, wie es das Gesetz von ihnen verlangt. Trotzdem sollte man im Internet mit persönlichen Daten vorsichtig sein, Spyware und manipulierte Websites (Phishing) stellen ausser Crackern eine grosse Gefahr dar.

# Überwachung durch Kundenkarten

Ich konnte durch gezielte Anfragen leider nur die Kundenkarten von Coop und Migros in Erfahrung bringen, da mir nur diese Karten zur Verfügung standen.

## Coop


### Allgemeine Geschäftsbedingungen

In den allgemeinen Geschäftsbedingungen (AGBs), welche auf www.supercard.ch einsehbar sind, macht sich Coop selbst grosse Einschränkungen:

> Aus dem System wird nicht ersichtlich, welcher Kunde welche Artikel oder Artikelgruppe einkauft.
>
> Wir speichern nebst Personalien der KarteninhaberInnen lediglich Ort und Betrag des Einkaufs sowie die generierten Superpunkte.
>
> Es werden keine individualisierten Warenkorb-Auswertungen erstellt aufgrund Ihrer Einkäufe mit der Supercard.

### Ergebnis der Anfrage

Als Antwort auf meine Anfrage per Brief bekam ich einen recht unpersönlichen Brief (ohne Unterschrift, mit Standarttext), in welchem mir folgende Informationen mitgeteilt wurden:

- Unsere Adresse
- Unsere Telefonnummer (Homenummer, keine Natelnummer, etc.)
- Die Supercard Nummer
- Unseren Kontostand per 2. Juni 2005

Coop hat sich demnach exakt an die allgemeinen Geschäftsbedingungen gehalten und benützt das Supercardsystem explizit nur für die Punktekalkulation.

Leider wurden mir **nicht alle Daten** (wie im DSG Art. 8.2ab vorgeschrieben) zugesandt. In den AGBs wird festgehalten, dass auch der Ort des Einkaufs inkl. Betrag gespeichert wird. Diese Informationen hätten mir ebenfalls zugesandt werden müssen.

Im Gegensatz dazu hat die Migros sich exakt an den oben genannten Artikel des DSG gehalten:

## Migros

### Allgemeine Geschäftsbedingungen

In den allgemeinen Geschäftsbedingungen (AGBs), welche auf www.m-cumulus.ch einsehbar sind, nimmt sich Migros folgende Rechte:

> Mit Ihrer Unterschrift gestatten Sie der Migros ausdrücklich, über die M-CUMULUS Karte erhaltene Daten für weitere Zwecke (Marketing, Auswertung, Statistiken) zu verwenden.
>
> Aufgrund Ihrer Einkaufsdaten werden wir z.B. in der Lage sein, Ihnen konkrete Angebote und Informationen (auch per Email) zukommen zu lassen, die für Sie von Interesse sein könnten.

### Ergebnis der Anfrage

Da ich persönlich keine M-Cumulus Karte besitze, wandte ich mich an meinen Mitschüler Jan Appl, welcher mir seine M-Cumulus Karte zur Verfügung gestellt (und nicht zu vergessen auch ein Teil seiner Privatsphäre gezeigt) hat. Dafür möchte ich mich an dieser Stelle recht herzlich bedanken.

Jan bekam ein ziemlich dickes, eingeschriebenes Couvert von der Migros, welches – wie ich glaube – wirklich alle Daten, welche über Jan Appl gesammelten Daten (Kundenstammdaten, Kassenzettel, Kundenkontakte und Aufträge) plus ein Begleitschreiben enthielt. In diesem wurde er auf folgende Sachverhalte aufmerksam gemacht:

- Auskunftsbegehren kam von mir (Andreas Ruckstuhl).
- Aus Datenschutzgründen werden die Informationen Jan Appl zugestellt.
- Die von der Migros gespeicherten Daten kommen aus zwei Quellen:
  - Bei der Anmeldung angegebene Informationen
  - Während der Verwendung der M-Cumulus Karte gesammelten Daten
- Falls Jan Appl Angebote bei Generali, Migrosbank oder anderen Cumulus-Programmpartnern profitiert habe, sind dort ebenfalls seine Kartennummer in Verbindung mit dem gekauften Produkt und/oder der gekauften Dienstleistungen gespeichert.

Auf jedem der ca. 120 A4 Seiten sticht dem Leser das Datenschutzgütesiegel der SQS (Schweiz. Vereinigung für Qualitäts- und Managementsysteme) ins Auge, welches ein Datenschutzgesetzgerechter Umgang mit Personen- und Kundendaten bestätigt. Da meine Lehrfirma selbst SQS zertifiziert ist (ISO9001), kenne ich die Auditverfahren und die Prüfung der vorgeschriebenen Dokumente, Arbeitsabläufe, etc. genau und kann bestätigen, dass dieses Gütesiegel vertrauenswürdig ist.

Auf dem Kundernstammdatenblatt werden unter anderem folgende Informationen aufgelistet:

- Name und Adresse, Geburtsdatum, Anrede, Telefonnummer, E-Mailadresse (falls angegeben) und das Internetpasswort für die M-Cumulus Website
- Eruierte Haushaltsgrösse (bei Jan Appl unbekannt)
- Sprache, Geschlecht
- Werbe-, Adress- und Sperrstatus
- Diverse Zeitstempel (Erfassungs-, Mutations-, Adressmutationsdatum, erster und letzter Einkauf)
- Gesamtumsatz
- Kundenattribut 1-10 (bei Jan Appl waren alle auf Status „0“)

Was die Kundenattribute 1-10 sind, beantwortete der Brief nicht. Auch ein mehrmaliges Nachfragen bei der M-Cumulus Hotline brachte keine Ergebnisse (Zitat „Darüber bin ich nicht informiert“ oder „Zu diesem Thema kann ich keine Angaben machen“).

Der grösste Teil der Ausdrucke (74 Seiten) bestand aus den „Cumulus- Kassenzettel“, in welchen exakt jeder Einkauf inkl. jeden Artikel und dazugehörigen Rabatt aufgelistet war. Ebenfalls ersichtlich war der genaue Zeitpunkt und der Ort des Einkaufs (Filiale und Kassennummer).

Weitere 26 Seiten befassten sich mit dem Ort des Einkaufs im speziellen. Wieder wurde jeder Einkauf mit Zeit, Datum und Ort aufgelistet. Diese Zusammenfassung nennt die Migros „Cumulus- Einkäufe (Kassenzetteltotal)“.

Der kleinste Teil der Ausdrucke (4 Seiten) waren den „Cumulus- Kundenkontakten und Aufträge“ gewidmet. Hier stand, wann welches Magazin an Jan Appl versendet wurde und welche Coupons er erhielt.

Laut einer Medienmitteilung der Migros im September 2004 haben in der Schweiz ca. 450'000 Personen die M-Cumulus Karte. Bei einer einfachen Kalkulation wird jedem die Datenflut ersichtlich: ca. 120 A4 Seiten Kundeninformationen multipliziert mit 450'000 ergibt bescheidene 54'000'000 A4 Seiten an Kundendaten. Das entspricht ungefähr einem Stapel von ca. 4950 Metern, das ist höher als der Mont Blanc (4790m)!

### Finanzierung

Die Finanzierung des M-Cumulus Programms (welches durch die Firma M-Cumulus Marketing Services AG durchgeführt wird) wird laut der Erfolgsrechnung 2002 der Migros durch den gesamten Konzern getragen. Genauere Informationen waren von Seiten der Migros leider nicht zu erfahren.

Im Gegensatz zu Migros gibt sich Coop zugeknöpft über die Finanzierung des Supercard-Programms. Ich konnte keine Informationen zum Thema Finanzierung und Supercard finden, ebenfalls konnte Google kein Jahresbericht von Coop finden.

Es ist jedoch wahrscheinlich, dass die Finanzierung über die Marketing und CRM Abteilung läuft, da diese die Kundenwünsche genauer untersuchen, um so besser die Kunden für sich und die eigenen Produkte gewinnen zu können.

### Gesetzliche Grundlagen

Die gesetzlichen Grundlagen für diese Art der Datensammlung durch Kundenkarten, wie sie die Migros betreibt, finden sich im DSG Art. 13.1:

> Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

Da jeder Besitzer einer M-Cumulus oder anderen Kundenkarte auf dem Antragsformular mit einem X die allgemeinen Geschäftsbedingungen akzeptiert (in welcher der Antragssteller dem Kartenherausgeber seine Einwilligung gibt), sind diese Datensammlungen erlaubt.

In Kritik geraten sind jedoch die speziellen Aktionen („diese Woche auf Artikel XYZ mit der Supercard 20% Rabatt“), da die Nutzung dieses Angebots eine Teilnahme am Kartenprogramm voraussetzen und der Kunde somit erpresst wird, seine Daten zugänglich zu machen.

## Zusammenfassung Kundenkarten

Wie man anhand dieser zwei Beispiele (Migros, Coop) erkennen kann, sind die angewandten Praxen unterschiedlich. Dies dürfte sich auch bei weiteren Anbietern von Kundenkarten wiederholen.

Grundsätzlich kann man jedoch sagen, dass die Verwendung der durch Kundenkarten gewonnenen Daten transparent ist und den gesetzlichen Anforderungen genügt.

# Überwachung im öffentlichen Verkehr

*Abb. 4: Überwacher Publikum (UePubl) in der Betriebsleitzentrale (BLZ) Zürich*

## Wo und wie wird überwacht?

Grundsätzlich werden an allen grösseren Bahnhöfen und in gewissen Regionalbahnen und Busbetrieben die Reisenden auf Schritt und Tritt von Videokameras überwacht. In begleiteten InterCitys und InterRegios wird dagegen konsequent auf Videokameras verzichtet, ebenfalls in der S-Bahn Zürich (ausgenommen die Strecke S10, welche von der SZU betrieben wird). Jedoch wird bereits breit diskutiert, ob eine Videoüberwachung in den S-Bahnen im Kanton Zürich eingeführt werden soll (u.a. im Kanton Tessin bereits Alltag).

Ein Piktogramm (ähnlich dem auf der Titelseite dieser Arbeit) am Eingang des Gebäudes oder des Zugs / des Busses zeigt dem Reisenden, ob er von einer Überwachungskamera überwacht wird.

Wie weit die Überwachung am Zürcher Hauptbahnhof geht, zeigt die Kamerakarte, welche viele Privatpersonen und Mitglieder des Vereins „*Big Brother Awards*“ zusammengestellt haben. Sie zeigt die unterschiedlichen Kamerastandorte und -Besitzer auf:

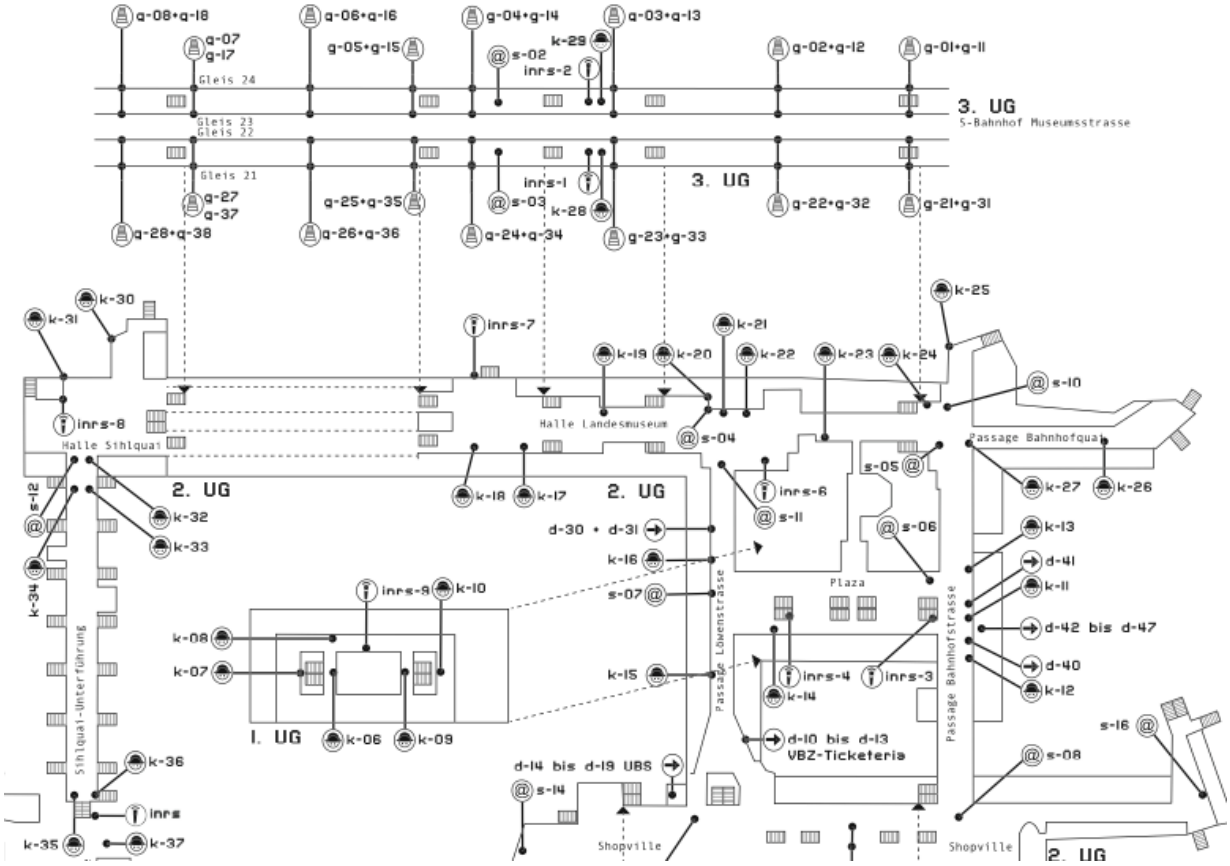



*Abb. 5: Ausschnitt der Kamerakarte Zürich HB von www.bigbrotherawards.ch*

**Hinweis:** Eine weitere Kamerakarte von Zürcher Kreis 4 ist ebenfalls auf der Website von „*Big Brother Awards*“ verfügbar.

## Interview

SBB CFF FFS

Im Anschluss an dieses kurze Vorwort finden Sie ein Interview mit Herrn Thomas Weibel, *Leiter Öffentliche Sicherheit* bei der SBB, welches via E-Mail geführt wurde.

An dieser Stelle möchte ich mich nochmals recht herzlich bei Herrn Weibel für seine Kooperation, seine Recherchen innerhalb der SBB und die ausführlichen Antworten bedanken, welche einen wesentlichen Beitrag zu dieser Arbeit leisteten!

### Zusammengestelltes Gespräch

*Wo werden die aufgezeichneten Daten in den Zügen, Bussen gespeichert?*

Laufend aufgezeichnete Daten werden je Reisewagen auf einer Blackbox aufgezeichnet.

*Wo werden die aufgezeichneten Daten in den Bahnhöfen gespeichert?*

Für diese Aufzeichnung gilt das gleiche Prinzip - vor allem in Hinblick für die Verwendung als Beweismittel. Es ist allerdings richtig, dass gewisse Sequenzen in den RailCity in den Zentralen auch live ausgewertet werden. (siehe Abb. 2)

*Wer hat Zugriff auf die aufgezeichneten Daten? Ist die zuständige Person mit dem Datenschutzgesetz vertraut?*

Zugriff auf die Blackbox und somit die Daten erfolgt nur durch die Bahnpolizei (Vereinbahrung durch die Bahnpolizei erfolgte im Rahmen des Datenschutzgesetzes). Die SBB ist im Sinne des Datenschutzgesetzes ein Bundesorgan. Für die Videoüberwachung wurde die SBB mittels einer bundesrätlichen Verordnung rechtsgenüglich legitimiert.

*Wie lange werden die Daten aufbewahrt?*

Aufgezeichnete Daten werden nach 24 Stunden automatisch überschrieben, bzw. gelöscht.

*Werden Datensicherungen erstellt, und wenn ja, wie werden diese verwaltet, bzw. vernichtet?*

Eine Datensicherung durch die Bahnpolizei erfolgt innerhalb von 24 Stunden und nur bei angezeigten und/oder bekannten Straftaten. Ausgewertete Daten werden den Behörden nur mit untersuchungsrichterlichem Ersuchen ausgehändigt.

*Zum allgemeinen Datenschutz: Welche aufgabenbezogenen Stellen haben wie Zugriff auf die generierten Daten (GA, Halbtax, Gleis 7, etc)?*

Hier gibt es folgende Punkte zu beachten:

- Fahrausweis- bzw. Schwarzfahrerdatenbanken sind völlig getrennt.
- Für Fahrausweise wie GA/Halbtax/Gleis 7 haben die beteiligten Transportunternehmen Zugriff
- Bei der SBB gibt es eine einzige Schwarzfahrerdatenbank. Zugriff dazu hat nur das Kompetenzzentrum Einnahmensicherung beim Personenverkehr.
- Weder Polizei noch Wohngemeinde oder andere Transportunternehmen haben Zugriff; ebenfalls haben Tarifverbunde (z.B. ZVV) keinen Zugriff.
- Die Daten bleiben zwei Jahre gespeichert.

Ich hoffe, Ihnen mit diesen Angaben dienen zu können und wünsche Ihnen für Ihre Arbeit viel Erfolg!

*Vielen Dank!*

# Überwachung durch Geldinstitute und Kreditkartenfirmen

*Abb. 6: Überwachungskamera am Bankomat*

### In der Bank, Bargeldbezüge

Aufgrund der Sicherheitskameras in jeder Bank und der Aufzeichnung der Videodaten wird jede Bewegung innerhalb der Kunden- und 24h Zone genauestens festgehalten.

Mitarbeiter, welche in der Kundenzone arbeiten, werden so ebenfalls überwacht.

Kameras im Bankomaten wie in Abb. 4 dargestellt dienen der Bank als genauere Überwachung dieses Geräts. Bei Kundenaussagen wie „Ich habe an diesem Tag hier kein Geld bezogen“ können so genau überprüft werden und ggf. die gemachten Bilder der zuständigen Polizeistelle als Beweis übergeben werden.

### Kontobewegungen

Wie bei meiner Anfrage (MigrosBank) per Brief vom 23. Mai ausgekommen war, müssen die Banken alle Kontobewegungen und Umsätze während mindestens 10 Jahren aufbewahren (siehe unten). Dazu gehören auch Ort des Bargeldbezugs oder des bargeldlosen Einkaufens.

### Bezahlung mit Kreditkarten

Verschiedene Personen nutzen Kreditkarten als Ersatz für Bargeld im In- und Ausland und als Bezahlungsmittel im Internet. Da jede Bewegung (vom Gesetzgeber verlangt) 10 Jahre aufgezeichnet werden muss, können aus den gewonnenen Rohdaten (Ort des Einkaufs, Produktgruppe, Preisklasse, etc.) durch Datamining bereits komplexe Persönlichkeitsprofile erstellt werden. Diese werden dann z.B. von Internetshops (prominentes Beispiel Amazon) verwendet, um den Kunden möglichst für ihn interessante Produkte aufmerksam zu machen.

Kritisch wird es dann, wenn die gesammelten Daten dazu verwendet werden, das Angebot speziell mit Reizen auszustatten, auf welche der Kunde (un-)bewusst anspricht und mehr kauft (siehe Abschnitt Bevormundung und Manipulation als Folge der Datenhaltung im Kapitel Datamining).

### Ergebnis der Anfrage an MigrosBank

Ich habe der MigrosBank (bei welcher ich zwei Konten besitze) ebenfalls ein Auskunftsbegehren geschickt. Innerhalb von drei Tagen sandte man mir einen persönlichen Brief (inkl. zwei Unterschriften), in welchem man mir mitteilte, dass sie folgende Daten von mir gespeichert haben:

- Name, Vorname und Wohnadresse
- Identitätskarte (fotokopiert)
- Geburtsdatum und Nationalität
- Basisvertrag mit Unterschriftenmustern vom Kontoinhaber und den bevollmächtigten Personen
- Administrative Daten vie Korrespondenzsprache, Versandinstruktionen, Daueraufträge, Lastschriftverfahren und Kontokarten
- Kontobezogene Daten wie Umsätze und Kontoabschlüsse müssen aufgrund gesetzlicher Bestimmungen während mindestens 10 Jahren aufbewahrt werden.

## Schlusswort

**Beeinträchtigt oder verbessert die heutige Überwachung unsere Lebensqualität?**

Beide Antworten sind richtig: Die Nachteile liegen auf der Hand: Überwachung auf Vorrat wie bei der Fichenaffäre schüren Ängste, durch Verminderung der Privatsphäre wird ein Menschenrecht gelockert (Recht auf Privatsphäre), durch Bevormundung und Manipulation der Kunden wird das Vertrauen in die Wirtschaft geschwächt, usw..

Die Vorteile sind ebenfalls klar: Wenn durch die heutige und zukünftige Überwachung Terrorakte verhindert und die organisierte Kriminalität vermindert werden kann, hat sich der Aufwand gelohnt. Natürlich sind auch kleinere Errungenschaften toll, wie z.B. die Schnellwahltaste am Bankomaten, welche uns den gewohnten Wunsch anbietet (wie immer; 100.- ohne Beleg?)...

Wir müssen nun dafür sorgen, dass ein gutes Gleichgewicht eingehalten wird, um die Vorteile weiterhin zu erhalten und trotzdem ein guter Schutz der Privatsphäre zu gewährleisten. Dazu gehört auch das Abschaffen von völlig überflüssigen Überwachungen (wie sie z.B. in Büros von gewissen Firmen Realität ist).

Ebenso müssen die Staaten und Firmen eine bessere Informationspolitik bezüglich der Datensammlungen entwickeln, denn nur wer transparent arbeitet, ist vertrauenswürdig.

Dies erreichen wir am besten, je mehr Personen sich über den Datenschutz und um die Überwachung Gedanken machen. Denn wo ein öffentliches Interesse ist, da ist auch das Interesse der Medien und somit wird diese Problematik auch öffentlich diskutiert.

In diesem Sinne:

**Stay tuned!**

# ANHANG

## Glossar

**A**

AGB ..... **A**llgemeine **G**eschäfts**b**edingungen

**B**

BÜPF ..... **B**undesgesetz betreffend **Ü**berwachung **P**ost- und **F**ernmeldeverkehrs

**C**

CIA ..... **C**entral **I**ntelligence **A**gency
CRM ..... **C**ustomer **R**elationship **M**anagement

**D**

DAP ..... **D**ienst für **A**nalyse und **P**rävention
DHCP ..... **D**ynamic **H**ost **C**onfiguration **P**rotocol
DSG ..... Bundesgesetz über den Datenschutz (**D**aten**s**chutz**g**esetz)

**E**

EDSB ..... **E**idgenössischer **D**aten**s**chutz**b**eauftragter
EJPD ..... **E**idgenössisches **J**ustiz- und **P**olizei**d**epartement
EMD ..... **E**idgenössischen **M**ilitär**d**epartement

**F**

FBI ..... **F**ederal **B**ureau of **I**nvestigation
Fedpol ..... Bundesamt für Polizei

**G**

GPDel ..... **G**eschäft**p**rüfungs**del**egation

**I**

IP ..... **I**nternet **P**rotokoll
ISP ..... **I**nternet **S**ervice **P**rovider

**N**

NSA ..... **N**ational **S**ecurity **A**gency

**P**

PUK ..... **P**arlamentarische **U**ntersuchungs**k**ommission

**R**

RFID ..... **R**adio **F**requency **Id**entification

**S**

SBB ..... **S**chweizerische **B**undes**b**ahnen AG
SND ..... **S**trategischer **N**achrichten**d**ienst
SQS ..... **S**chweiz. Vereinigung für **Q**ualitäts- und Management**s**ysteme

**V**

VBS ..... **V**erteidigung – **B**evölkerungsschutz – **S**port

**W**

WEP ..... **W**ired **E**quivalent **P**rivacy (erste Verschlüsselungstechnologie für WLAN)
WLAN ..... **W**ireless **L**ocal **A**rea **N**etwork (kabelloses Computernetzwerk)

**Z**

ZVV ..... **Z**ürcher **V**erkehrs**v**erbund

## Bildreferenz

Die Abbildungen und Fotos habe ich von den folgenden Quellen bezogen:

Abb. 1 (Umfrage) .....Screenshot des Umfrageergebnisses am 5. Juli 05 um 23:00

Abb. 2 (Bodenstation) .....Verestar Bodenstation in Leuk (VS)
Quelle: Website der Schweizerischen Raumfahrt-Vereinigung
www.srv-ch.org

Abb. 3 (Mobilfunk) .....Screenshot des Programms CellTrack auf meinem Nokia 6600, welches sich zum Zeitpunkt der Aufnahme bei mir zu Hause in Neftenbach befand.
Das Programm zeigt die Informationen an, die es von den jeweiligen Antennen empfängt.

Abb. 4 (Überwach. SBB) ..Von mir aufgenommenes Foto im BLZ Zürich, Langstrasse, 2. Stock während eines Vor-Ort Einsatzes meines Lehrbetriebs (Erneuerung Telekommunikationsanlage).
Die 16 Monitore zeigen abwechslungsweise Bilder von den Bahnhöfen Zürich HB, Zürich Stadelhofen, Zürich Hardbrücke, Stettbach.

Abb. 5 (Kamerakarte) .....Kamerakarte Zürich HB
Quelle: Website von Big Brother Awards
www.bigbrotherawards.ch

Abb. 6 (Bankomat) .....Von mir aufgenommenes Foto in der Migrosbank Winterthur, beim Bankomat in der 24h Zone.

## Quellenverzeichnis

Folgende **Antworten** habe ich als Quellen für diese Arbeit verwendet:

- Auskunftsbegehren (Orange, Migros, MigrosBank, Coop, Cablecom)
- Antworten auf Fragen (SBB, Big Brother Awards)

Folgende **Internetadressen** habe ich als Quellen für diese Arbeit verwendet:


- Admin.ch: Diverse Gesetzestexte
  http://www.admin.ch
- Big Brother Awards: Allgemeine Informationen zum Thema Überwachung
  http://www.bigbrotherawards.ch
- Parlament.ch: Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte
  http://www.parlament.ch/print/ed-pa-gpd-onyx-d.pdf
- Eidgenössischer Datenschutzbeauftragter
  http://www.edsb.ch/d/fragen/rechte/index.htm
- SFDRS; SF-Spezial Sendungen „Alles unter Kontrolle“
  http://real.xobix.ch/ramgen/sfdrs/vod/sfspezial/sfspezial_20041129.rm
  http://real.xobix.ch/ramgen/sfdrs/vod/sfspezial/sfspezial_20041202.rm
- Tor.at: Artikel „Öffnet Swisscom- Outsourcing Echelon Tür und Tor?“
  http://www.tor.at/resources/focus/telepolis/echelon/heise.de/tp/deutsch/special/ech/4326/1.html
- Uni Zürich: Vortrag „Sicherheit und Datenschutz“
  http://www.ifi.unizh.ch/egov/it_engineering_04/Sicherheit_Datenschutz/Sicherheit_Datenschutz.html
- Weltwoche: Artikel „Was sagen Sie jetzt?“ zum Thema Onyx
  http://www.weltwoche.ch/artikel/?AssetID=10344&CategoryID=60
- Wikipedia: Diverse (aber vor allem technische) Informationen
  http://de.wikipedia.org
- WoZ Online: Artikel „Mister Echelon im Onyx-Land“
  http://www.woz.ch/archiv/old/02/17/6573.html