Privacy – The right to be left alone

Andreas Müller
D-ITET
andrmuel@ee.ethz.ch

Daniel Furrer
D-INFK
dfurrer@student.ethz.ch

Zusammenfassung

Gestützt auf Artikel 8 des Datenschutzgesetzes haben wir verschiedene Unternehmen und Staatsstellen aufgefordert, uns die über uns gesammelten Daten zu senden. Anhand dieser Daten haben wir uns überlegt, was ein Unternehmen für Informationen über uns herausfinden könnte. Zusätzlich haben wir einige allgemeine Grundlagen zu Datenschutz und Privatsphäre zusammengetragen.[1]

[1] Dieser Bericht entstand im Rahmen einer Projektarbeit in der Vorlesung ≪Freie Software - Nachhaltigkeit in der Wissensgesellschaft≫ WS 05/06 von M. Dapp.

Privacy is the right to be let alone.
– Thomas M. Cooley

Inhaltsverzeichnis

1 Einleitung

1.1 Geschichte

Während die Daten über eine Person gesammelt werden früher auf wenige, wichtige Ereignisse beschränkt waren zeichnet sich in den letzten Jahren eine resante Entwicklung zu immer weitreichenderen Datenbanken ab. Einzelne, gedrukte Dokumente wurden ersetzt durch vernetzte Datenbanken, die sich in sekundenschnelle abgefragen und auswerten lassen. Insbesondere durch das Internet können Daten vermehrt auch unbemerkt zusammengetragen werden. Es ist ein regelrechter Datenmarkt entstanden, denn die Firmen können sich durch mehr wissen über eine Person einen marketingtechnischen Vorteil ergattern und andere Firmen werden quasi gezwungen dem Beispiel zu folgen. Die Entwicklung wird in Zukunft also noch weiter diese Richtung gehen. Deshalb ist es wichtig die Möglichkeiten und Gefahren die daraus Resultieren genau zu beobachten.

1.2 Warum braucht mensch eine Privatsphäre?

Bei Unterhaltungen über Datenschutz muss man oft Aussagen hören wie "Warum sollte mich Überwachung stören, ich habe ja nichts illegales getan und nichts zu verstecken". Bedenkt man, dass Menschen in Sendungen wie BigBrother bereit sind, volkommen auf ihre Privatsphäre zu verzichten, einzig aufgrund der Hoffnung, ein wenig Bekanntheit zu erlangen, so scheint die Frage berechtigt.

Andererseits lassen sich aber schnell vielseitige Gründe finden, warum auch ein Bürger der nicht mit dem Gesetz in Konflikt steht seine Privatsphäre schützen sollte:

- Machmal ist Anonymität die einzige Möglichkeit zur freien Meinungsäusserung. Dies zeigt sich z.B. in China, wo offene Kritik gegen die Regierung äusserst gefährlich ist, oder anhand der Sekte Scientology, die sich wegen sehr aggresiver Repression nur schwer öffentlich kritisieren lässt.
- Überall wo Minderheiten diskriminiert werden, können diese durch Privatsphäre geschützt werden. Das extremste Beispiel dazu ist vermutlich Deutschland während dem zweiten Weltkrieg, wo es für viele Juden tödlich war, dass der Staat nur schon über ihre Religion informiert war.
- An öffentlicher Überwachung wird auch immer wieder kritisiert, dass damit alle als verdächtig eingestuft werden. Dies widerspricht dem demokratischen Grundsatz der Unschuldsvermutung.
- Genaue Informationen über eine Person ermöglichen es einem Unternehmen, personalisierte Werbung und Propaganda zu verwenden. Dies ist gefährlich, da dadurch für jeden Menschen eine persönliche Realität entsteht.
- Ein sehr lästiges Problem ist inzwischen auch Werbung und Spam. Dieses Problem kann teilweise durch den Schutz der persönlichen Daten bekämpft werden.
- Werden Technologien wie z.B. Verschlüsselung nur von Kriminellen verwendet, so werden diese auf Dauer illegal.

Als Grund für Überwachung wird – vor allem seit dem 11. September – immer wieder die Sicherheit aufgeführt. Es ist aber fraglich, ob z.B. mit

einer Überwachungskamera die Sicherheit effektiv gefördert wird, oder nur ein Scheingefühl der Sicherheit.

Bedenklich ist dabei, dass im Namen der Sicherheit immer mehr bürgerliche Freiheiten aufgegeben werden. Bereits Benjamin Franklin meinte dazu sehr deutlich: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[20]

1.3 Gesetze

Gesetze zum Datenschutz sind in der systematischen Rechtssammlung des Bundes unter SR 235 [3] einzusehen. Die Gesetze sind verständtlich geschrieben und sehr lesenswert. Den Datenschutz bestimmt in erster Linie das DSG [4]. Problematisch ist allerdings die mangelhafte Einhaltung der Gesetze und das oft fehlende Bewusstsein für Datenschutz in der Bevölkerung ("habe ja nichts zu verstecken"). Ein Unternehmen hat kaum Strafen oder Kundenverlust zu befürchten, wenn z.B. Daten "versehentlich" oder "aufgrund eines Computerfehlers" zu lange gespeichert wurden (bekanntlich sind ja sowieso an allen Unannehmlichkeiten für Kunden einzig die Computer schuld).

Des weiteren gibt es den eidgenössischen Datenschutzbeauftragten [5]. Im Moment ist dies Hanspeter Thür, mit einem 20-köpfigen Team. Diese Personen setzen sich immer wieder kompetent für Datenschutz ein; es ist aber zweifelhaft, ob ein 20-köpfiges Team alle Unternehmen und Staatsstellen der Schweiz überwachen kann, während es sich nebenbei noch um die Sorgen einzelner Bürger kümmert.

Zusätzlich gibt es auch kantonale Gesetze und Datenschutzbeauftragte, für Zürich z.B. mit Homepage unter [6]. Je nach Kanton können diese aber auch – wie z.B. im Aargau – ganz fehlen.

1.4 Die Sammler und Jäger

1.4.1 Staat

Der Staat ist stets in einem gewissen Masse an Kontrolle über seine Bürger interessiert. Während ohne jegliche Kontrolle eine Anarchie bestehen würde, entsteht andererseits bei zuviel Kontrolle ein totalitärer Überwachungsstaat. Es muss bei jeder Massnahme einzeln abgeschätzt werden, ob diese im öffentlichen Interesse liegt und verhältnismässig ist, wie es die Bundesverfassung, Artikel 5^2 vorschreibt, oder ob sie Bürgerrechte – z.B. Recht auf Privatsphäre, Artikel 13 der Bundesverfassung – zu stark einschränkt.

Zur Überwachung werden z.B. die Rahmendaten elektronischer Kommunikation protokolliert. Einblick in diese Daten sowie Überwachung der Kommunikation selbst ist aber nur nach richterlichem Beschluss erlaubt (SR 720.1 Art. 7 [9]).

1.4.2 Unternehmen

Unternehmen interessieren sich in erster Linie zu Werbezwecken für Kundendaten, da personalisierte Werbung deutlich effizienter ist als allgemeine Werbung.

Zur Datenjagd werden vor allem Kundenkarten eingesetzt, mit denen nicht nur die Kunden gebunden werden, sondern auch ihr Einkaufsverhalten genaustens aufgezeichnet werden kann. Zur Adressbeschaffung sind

auch Wettbewerbe immer wieder beliebt. Mit wenig Aufwand und geringen Ausgaben für Preise gewinnt ein Unternehmen die Adressdaten aller Teilnehmer. Sehr interessant sind auch die sozialen Beziehungen zwischen Kunden. Um diese herauszufinden – und um neue Kunden zu gewinnen – gewähren Unternehmen oft Rabatte bei Anwerbung von Neukunden durch bestehende Kunden. Für die Offenlegung der sozialen Beziehungen bieten Unternehmen durchaus auch Dienstleistungen gratis an, wie z.B. bei Gmail [7] der Fall.

1.4.3 Arbeitgeber

Bei Arbeitgebern steht die Kontrolle der Arbeitnehmer im Vordergrund. Dazu steht - nebst persönlicher Kontrolle - von Telefonüberwachung über Keylogger bis zu Überwachungskameras ein breites Spektrum an technologischen Mitteln zur Verfügung.

2 Die von uns angeschriebenen Unternehmen und Staatsstellen

Um herauszufinden, was für Informationen Unternehmen über uns sammeln, haben wir verschiedene angeschrieben. Dazu waren auch die Musterbriefe [8] des Datenschutzbeauftragten hilfreich. Die Unternehmen sind dank DSG, Artikel 8 [4] verpflichtet, uns Einsicht in unsere Daten zu gewähren.

2.1 Die Armee (PISA Datenbank, Andreas)

Eine Mehrheit der Schweizer Männer und ein kleiner Teil der Frauen rückt irgendwann im Leben ins Militär ein. Schon aufgrund der grossen Anzahl Personen ist Datenschutz hier also wichtig. Geregelt ist die Datenbearbeitung der Armee im Militärgesetz [10], Art. 146-148. Im VmK [11], Art.32 und Art. 33 sind die gesetzlichen Grundlagen für das Personal-Informations-System der Armee (PISA) festgelegt.

Auf Anfrage rückt die Armee ohne Umstände die im PISA gesammelten Daten raus. Diese enthalten u.a. die im Militär sehr beliebte AHV-Nummer, Name und Adresse, Beruf, allfällige Kaderempfehlungen, Funktion in der Armee, Grade mit Datum der Beförderungen, Einteilungen, Entscheide zur Taugklichkeit, Gerichtsurteile wie z.B. Verweise, geleistete und zu leistende Diensttage, Informationen über abgegebene Ausrüstung, Wohnorte, militärische und zivile Spezialausbildungen, Sprachkentnisse sowie Informationen über Führerausweise. Interessantes Detail: Laut Auskunft der Armee beherrsche ich als einzige Fremdsprache Italienisch. Tatsächlich spreche ich kein Wort Italienisch, aber selbstverständlich Englisch und Französisch. Pikant ist dies zusätzlich, weil die Armee laut VmK [11] Art. 22^3 (Anhang mit Daten: [12]) zur Erhebung von Daten über Sprachkentnisse ohne Einwilligung der Betroffenen gar nicht berechtigt ist.

Keine briefliche Auskunft (persönliches Erscheinen nötig) wird über die medizinischen Daten gegeben. Gerade die medizinische und psychologische Datenbank MEDISA (gesetzliche Grundlagen im VMBDD [13]) wurde vor allem seit der neuen, dreitägigen Rekrutierung (die ich selbst nicht durchlaufen habe) immer wieder heftig kritisiert, da im grossen Stil teilweise sehr intime Daten gesammelt und von diversen Personen eingesehen werden können (Datenkategorien und -benutzer sind aufgeführt im

Anhang zu MEDISA, [14]).

2.2 Conrad (Andreas)

Die schnellste Antwort kam vom Elektronikdistributor Conrad, gerade mal acht Tage nach Versand des Auskunftsbegehrens. In der Datenbank von Conrad wird laut eigener Aussage nur die Anschrift und die Telefonnummer, sowie die eMail-Adresse gespeichert. Verwendet werden diese Daten zur Bestellabwicklung sowie zu Marketing- und Marktforschungszwecken. Die Tatsache, dass man mit einer Anschrift und einer eMail-Adresse wohl nicht viel Marktforschung betreiben kann, lässt vermuten, dass zumindest auch die Daten der bestellten Artikel verarbeitet werden – allenfalls in anonymisierter Form und ohne personenbezogene Speicherung.

2.3 SBB (Andreas)

Die SBB schreiben, sie würden in ihrer Kundendatenbank lediglich Name, Adresse, Geburtsdatum, Telefonnummer, Art und Dauer des Abos, sowie ein Foto speichern. Laut SBB Datenschutzbeauftragtem, Beat Gattlen, sind die einzigen exteren Empfänger dieser Daten die Hersteller der Abos.

2.4 eBay (Andreas, Daniel)

Das international tätige Unternehmen eBay schreibt, es würden lediglich Mitgliedsname, Name, Adresse, Geburtsdatum und Telefonnummer, sowie Daten über die getätigten Transaktionen gespeichert (denn “eBay ist aufgrund gesetzlicher Vorschriften verpflichtet, diese Daten zu speichern“). Eine Übermittlung dieser Daten in die USA sei nötig, um weltweiten Handel zwischen den Mitgleidern zu ermöglichen. Des weiteren wird auf die Datenschutzgrundsätze von eBay verweisen.

Die Antwort von eBay macht überhaupt einen sehr seriösen Eindruck. Der Brief vermittelt das Gefühl, dass die persönlichen Daten bei eBay gut aufgehoben sind. Dieser Eindrück verflüchtigt sich aber leider bei genauerer Betrachtung sehr schnell und weicht dem unangenehmen Gefühl, dass alle Daten ziemlich gut verwertet werden.

Die ersten Zweifel kommen spätestens dann, wenn man auf der Seite von eBay auf “Datenschutzerklärung“ klickt. Hier erwartet den Nutzer nämlich nicht etwa das Versprechen von eBay, die Daten sorgsam zu schützen, sondern es werden unter dem Titel “Einwilligung in die Verarbeitung meiner personenbezogenen Daten“ insgesamt neun Punkte aufgelistet, in denen der Nutzer eBay ermächtigt hat, seine Daten zu verarbeiten. Dies ist die gleiche “Datenschutzerklärung“, der jeder Nutzer bei der Anmeldung zustimmt – und sie ist auch zu diesem Zeitpunkt nur über einen irreführenden Link, beschriftet mit “Datenschutzerklärung“, zu finden.

Mühe bei der Glaubwürdigkeit von eBay bereitet daneben die wiederholte Aufforderung von eBay selbst sowie von Paypal (welches von eBay aufgekauft wurde), die persönlichen Kreditkartendaten zu übermitteln. Gerade bei Paypal entsteht der Eindruck, Paypal könne ohne Kreditkarte nicht sinnvoll genutz werden – obwohl sowohl Paypal als auch eBay problemlos mit normalen Postüberweisungen genutzt werden kann. Es drängt sich die Frage auf, ob eBay dabei am Komfort der Kunden interessiert ist, oder ob einfach der Geldfluss bei Kreditkarten besser verfolgt werden kann.

Dubios mutet auch der vorletzte Satz aus dem Brief von eBay an: “eBay arbeitet mit Strafverfolgungsbehörden in Form der Datenherausgabe zusammen, soweit die gesetzlichen Voraussetzungen hierfür vorliegen.“ Es ist kaum anzunehmen, dass damit nur die Strafverfolgungsbehörden der Schweiz gemeint sind – stimmt der Nutzer bei der Anmeldung doch ausdrücklich der Übermittlung seiner Daten in die USA zu und willigt weiter unten ein, dass eBay “soweit dies erforderlich ist, [die Daten] an Strafverfolgungs- und Aufsichtsbehörden zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten übermittelt, soweit die Übermittlung [der Daten] an Dritte nicht aufgrund eines Gesetzes [auch ohne Einwilligung] erlaubt ist.“ [19]

2.5 Migros (Daniel)

Ebenfalls sehr schnell geantwortet hat die Migros, welche auch als einziges Unternehmen einen eingeschriebenen Brief verschickt hat. Von ihr haben wir die umfangreichste und vollständigste Antwort erhalten. Die Migros hat auf alle gestellten Fragen geantwortet. Die Daten umfassen unter anderem die bei der Anmeldung für das Cumulus Angebot anfallenden Daten, insbesondere Adresse, Geschlecht, Geburtsdatum und Haushaltsgrösse der angemeldeten Person. Zusätzlich erhielten wir auf 120 Seiten sämtliche Kassenzettel inklusive Einzeleinkäufe (u.a. Datum, Zeit, Filiale, Einkaufswert und Produktname) über 15 Monate[1] zurück und die Kassenzettel-Totale, welche die Migros über 3 Jahre zurück aufbewahrt. Aber auch der Gesamtumsatz, das Registrierungsdatum, das Datum des letzten Einkaufes und die meistbesuchte Filiale werden verzeichnet.

Insgesamt hinterlässt die Migros trotz der Sammelwut einen relativ guten Eindruck. Die Migros informiert auf ihrer Website vorbildlich über die Auskunfts- und Löschungsrechte, sowie den Umfang der gesammelten Daten. Ein wenig lächerlich erscheint der Hinweis auf das Good-Priv@cy Label [22]. Alles, was dieses Label zertifiziert ist, dass “der Umgang [mit den Daten] vollumfänglich den gesetzlichen Anforderungen[2] und den weitergehenden Migros-internen Datenschutzregeln[3] entspricht“ [22], [23]. [23].

2.6 Ricardo (Daniel)

Auf das erste Auskunftsbegehren hat Ricardo geantwortet, dass keine Daten vorliegen, wobei sich aber nach einigen weiteren Abklärungen herausgestellt hat, dass die Daten bei Ricardo nur fehlerhaft abgelegt waren. Die Verantwortliche bei der ricardo.ch AG hat mir dann einen Link zu einer Seite auf der man sich sein vergessenes Passwort zustellen lassen kann geschickt.

Obwohl sich die Verantwortliche nachdem ich ihr mitgeteilt hatte, dass wir gerne eine völlig andere Auskunft möchten noch um eine Abklärung bemüht hatte haben ich daraufhin keine Zeit mehr gehabt noch weiter nachzuhaken. Es scheint als habe Ricardo zum ersten Mal ein Auskunftsbegehren gesehen.

[1] Die Angabe im Brief, den wir erhalten haben stimmt seltsamerweise nicht mit den auf der Website (14 Monate) überein.

[2] Ironisch nicht nur, weil dies hoffentlich kein Zertifikat braucht, sondern auch weil man es genau umgekehrt verstehen kann – wenn Migros die Gesetze exakt einhält, kann das ja auch heissen, dass sie die maximale Menge an Daten sammeln, die das Gesetz noch zulässt.

[3] Diese sind leider nirgends ersichtlich. Eine entsprechende Anfrage an Migros wurde freundlich beantwortet und verdient einen eigenen Abschnitt (siehe Anhang A).

2.7 Überblick

Zunächst können wir festhalten, dass wir von allen Stellen, die wir angeschrieben haben innerhalb einer vernünftigen Frist eine Antwort erhalten haben. Ob dies davon abhängig war, dass wir alle Anfragen eingeschrieben verschickt haben sei dahingestellt.

Die Antwortbriefe entsprachen aber nicht immer unseren Vorstellungen. So scheint beispielsweise der Brief an eBay von der Marketingabteilung beantwortet worden zu sein, statt von der Rechtsabteilung.

Der Umfang der gesammelten Daten könnte kaum unterschiedlicher sein. Während einige Unternehmen nur die allernötigsten Daten behalten (SBB, Conrad) gibt es andere (Migros), die praktisch alle Daten, die irgendwie anfallen, sammeln.

3 Auswertung der Daten

3.1 Disclaimer

Die folgenden Abschnitte sind lediglich Ideen und Gedankengänge. Wo nicht anders erwähnt, behaupten wir ausdrücklich nicht, dass ein Unternehmen diese Ideen umsetzt, sondern wir wollen lediglich die Möglichkeiten aufzeigen.

3.2 Data-Mining

Auf den ersten Blick erscheint die Sammelwut von Unternehmen absurd – wieso sollte es die Migros so sehr interessieren, wann ein Kunde eine Pizza einkauft. In der Tat sind diese Daten in der Rohform ziemlich wertlos. Hier kommt aber eine Technologie namens Data Mining [27] ins Spiel. Das Ziel von Data Mining ist es, durch die Analyse grosser Mengen an sich uninteressanter Daten, Muster zu erkennen und dadurch interessantere Informationen zu gewinnen. Die immer billigere Verfügbarkeit von Rechenleistung und Speicherplatz macht Data-Mining zu einem mächtigen Werkzeug.

3.3 Mögliche Zieldaten

3.3.1 Einkommen

Im Falle von Migros ist es z.B. denkbar, dass durch Auswertung der Einkaufsgewohnheiten eine ziemlich genaue Schätzung des Einkommens gemacht wird. Jemand, der stets M-Budget Produkte kauft, hat mit grosser Wahrscheinlichkeit ein niedrigeres Einkommen als jemand, der oft teures Fleisch einkauft. Ausserdem wird jemand, der auf seine Ausgaben achten muss wohl auch eher auf Aktionsangebote achten. Gerade ein Unternehmen wie Migros, dass sowohl Nahrungsmittel in diversen Preissegmenten, als auch reine Luxusgüter wie z.B. Unterhaltungselektronik verkauft, sowie ganze Reisen anbietet (Hotelplan), hat viele Möglichkeiten zur Schätzung der Kaufkraft von Kunden. Am einfachsten geht dies allerdings, wenn ein Kunde ein Konto bei der eigenen Bank hat (Migrosbank).

3.3.2 Arbeit

Direkt verbunden mit dem Einkommen ist die Arbeit. Es ist z.B. denkbar, aufgrund der Einkaufszeiten darauf zu schliessen ob jemand arbeitslos ist.

Kauft jemand unter der Woche regelmässig ein, so kann vermutet werden, dass diese Person keiner geregelten Arbeit nachgeht. Offensichtlich wäre eine solche "Einzelauswertung" sehr spekulativ und wenig nützlich, aber es darf nicht vergessen werden, dass ein Unternehmen möglicherweise eine sehr grosse Datensammlung hat. Aus der Kombination vieler solcher Puzzleteilchen kann deshalb ein sehr genaues Bild entstehen.

Zur Bestimmung der Art von Arbeit, welche ein Kunde ausübt, wäre es des weiteren möglich, zu überprüfen ob die jeweilige Person viele Büroartikel sowie bürotaugliche Kleidung und Kravatten einkauft, oder ob öfters Arbeitskleidung eingekauft wird, und welche.

3.3.3 Zivilstand

Nicht besonders schwer sollte auch das herausfinden des Zivilstandes sein. So bietet allein schon die Anzahl konsumierter Fertigpizzas einen guten Ausgangspunkt zur Beantwortung der Frage, ob ein Kunde Single ist. Vielleicht wäre es sogar denkbar, durch Veränderungen in den Essgewohnheiten auf Veränderungen in einer Beziehung zu schliessen. Eine solche Information wäre sicherlich werbetechnisch bestens auswertbar.

Problemlos denkbar ist auch die Feststellung, ob eine Familie Kinder hat und welches Alter diese haben. Während bei häufigem Windelkauf mit grosser Sicherheit Kleinkinder in einem Haushalt leben, kann z.B. beim Einkauf von PC-Spielen auf ältere Kinder geschlossen werden. Simpel wäre auch die Bestimmung der Gesammtmenge eingekaufter Esswaren, woraus sich ziemlich genau die Anzahl Personen in einem Haushalt ablesen lässt.

3.3.4 Gesundheit

Sehr pikant ist wohl die Lebenserwartung. Diese sollte sich Aufgrund der durchschnittlich eingekauften Menge von Raucherwaren, Alkohol und Fastfood – gegenüber Sportartikeln und Gemüse – zumindest grob bestimmen lassen. Zur genaueren Bestimmung wären wohl Daten vom Arzt nötig, wobei heute aber der Datenhandel zwischen Ärzten und Unternehmen dank Datenschutzgesetzen noch absolut undenkbar ist. Es darf diesbezüglich aber gespannt auf Dinge wie z.B. RFID Chips gewartet werden, die z.B. Gesundheitsdaten direkt "im Mensch" speichern könnten.

Abnehmer von Daten zur Lebenserwartung wären wohl in erster Linie Versicherungen und Krankenkassen – so ist es z.B. denkbar, dass Nichtraucher niedrigere Krankenkassenprämien bezahlen würden. Ob dies nicht gar positiv wäre, ist allerdings diskutierbar. Angesichts der aktiven Selbstzerstörung von Rauchern könnte einem solchen Vorgehen zumindest eine gewisse Berechtigung nicht abgesprochen werden.

3.3.5 Politische Ausrichtung

Vor allem für politisch aktive Unternehmen ist die Weltanschauung und die politische Ausrichtung ihrer Kunden sehr interssant. Diese ist wohl eine der schwieriger zu erhaltenden Informationen. Hat ein Unternehmen allerdings Grössen wie Einkommen, Familienstand und Wohnort eines Kunden bestimmt, so sollte sich mit ein wenig Statistik auch die politische Ausrichtung ermitteln lassen.

Sehr bedenklich ist in diesem Zusammenhang die Möglichkeit, personalisierte Wahlkampfpropaganda zu betreiben und Bürger gezielt mit (Des-)informationen zu versorgen. Es wird möglich, eine Bevölkerungsschicht

mit gezielten Wahlversprechungen zu beeinflussen, während diese einer anderen Bevölkerungsschicht vollkommen verborgen bleiben.

Konrad Becker schreibt dazu in seinem Buch "Die Politik der Infosphäre" [2] in düsterer Vorausahnung:

> Im Zuge der Privatisierung von staatlichen Einrichtungen und des Auslagerns von staatlichen Leistungen in die Privatwirtschaft kommt es allerdings zu einer Konvergenz des staatlichen und wirtschaftlichen Datensammelns und zu einer Integration von Daten, welche die politische und wirtschaftliche Repräsentation von Personen ununterscheidbar werden lässt. In der Konsequenz führt dies zur Anti-Utopie eines Citizen-as-Customer, in der Konsum und politische Partizipation ein und dasselbe sind, sodass die Politik in sich selbst zusammenbricht und als Karikatur ihrer selbst fortbesteht.

3.4 Zusammenfassung

Es zeigt sich, dass sich bereits mit einigen einfachen Überlegungen diverse Informationen finden lassen. Damit lässt sich halbwegs erahnen, was für Informationen durch intensiveres Data-Mining – mit ein wenig mehr finanziellem und zeitlichem Aufwand und unter Einsatz von Computern zur Datenanalyse – gefunden werden könnten. Computerprogramme zu diesem Zweck sind kommerziell erhältlich, z.B. Knowledge Server [31], Enterprise Miner [32] oder Scenario [33] (Beispiele aus [2]).

Das Ergebnis – möglichst detailierte Personendaten – ist ein wertvolles Gut, mit dem Direktmarketingfrimen wie Schober [30] Millionen verdienen. Dies wurde in der Sendung Kassensturz vom 10.1.2006 [29] ausführlich thematisiert.

4 Selbstschutz

Der Schutz der Privatsphäre ist stets mit einem gewissen Aufwand verbunden. Menschen, die die eigenen Daten schützen möchten – dieser Text hat dazu hoffentlich angeregt –, können aber auch ohne übermässige Zeitinvestition schon einiges erreichen:

- Auf Kreditkarten und Kundenkarten sollte verzichtet und stattdessen Bargeld eingesetzt werden
- eMails sind im Normalfall von Provider und allen Servern ziwschen Sender und Empfänger lesbar (vergleichbar mit einer Postkarte). Es ist vorteilhaft, eMails zu verschlüsseln und digital zu signieren, was z.B. mit GPG [24] möglich ist. Durch den Aufbau eines Web of Trust werden allerdings auch die eigenen sozialen Beziehungen teilweise offengelegt, da das Web of Trust für alle einsehbar ist [26]
- Falls doch Bedarf nach einer Super- oder Cumulus-Card da ist, bietet Bert Setzer [28] eine interessante Alternative
- Beim Versand von Dateien sollte darauf geachtet werden, dass nicht unabsichtlich zusätzliche Informationen versendet werden. Die Verwendung von offenen Formaten kann dabei hilfreich sein.
- Für Onlineangebote sollten – schon zum Schutz vor Spam – möglichst Wegwerfemailadressen verwendet werden. Solche sind z.B. bei Spamgourmet [25] erhältlich.

- Wo zu detailierte Angaben von Daten verlangt werden ist es am einfachsten, falsche Angaben zu machen (lügen!).
- Besteht bei einem Unternehmen der Verdacht, es könnte Daten weitergeben, so kann es helfen, einen zweiten Vornamen zu erfinden und anzugeben. Wird jeweils nur ein zweiter Vorname pro Unternehmen verwendet, so kann im Fall von unerwünschter Werbung sofort festgestellt werden, welches Unternehmen verantwortlich ist (da die Adresse den zweiten Vornamen enthält).
- Unternehmen und je nach Umständen auch Staatsstellen sind verpflichtet, gesammelte Daten auf Wunsch zu löschen.
- Gegen Werbung kann eine Sperrung der Adresse beim SDV [34] helfen. Ausserdem können Direktmarketingverbände angeschrieben werden, mit der Aufforderung, gesammelte Daten zu löschen.

Weitere Infos finden sich bei der EFF [16], dem CCC [15], im Buch von Konrad Becker [2], auf der Seite der BigBrother Awards [17], im Beobachter [18], sowie auf Seiten des Bundes [3], [5], [6]. In der Systematischen Rechtssammlung sind u.A. folgende Gesetze von Interesse:

- Fernmeldegesetz (z.B. 7. Kapitel: Fernmeldegeheimnis) [35]
- Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [36]
- Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS) [37]
- Verordnung über das Staatsschutz-Informations-System (interessant ist z.B. Art. 4) [38]
- Bundesgesetz über die Verwendung von DNA-Profilen [39]
- Verordnung über die Nachrichtendienste im VBS (Übersicht) [40]
- Verordnung über Massnahmen zur Wahrung der inneren Sicherheit (Inlandsnachrichtendients DAP) [41]
- Bundesgesetz über die Armee und die Militärverwaltung, Art. 99 (Militärischer Nachrichtendienst) [42]

A Antwort von Migros

Eine Anfrage an Migros nach den weitergehenden Migros-internen Datenschutzregeln ergab eine interessante Antwort. Diese soll den Lesern nicht vorenthalten bleiben (sorry, liebes Migros-Team – aber da kann ich nicht widerstehen).

A.1 Das eMail

```
Sehr geehrter Herr Müller

Besten Dank für Ihr Interesse an M-CUMULUS. Gerne erläutern wir
Ihnen noch etwas genauer unsere Definition der internen
Datenschutzregeln:

- Im Direct Marketing legen wir offen, woher die Adressen kommen.
- Daten werden nur mit einer hohen Verschlüsselung verschickt
- Wir betreiben keine Datenanreicherung mit externen Daten. Es
  wird nur das abgelegt, was bei der Nutzung der Konten anfällt.
- Wir arbeiten nur mit Agenturen, die im SDV (Schweiz. Direct
  Marketing Verband) Mitglied sind.
- Wir haben nur einen kleinen Benutzerkreis, der Zugang zu den
  Daten hat.

Für weitere Fragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse
[Name]
CUMULUS Marketing Services

-----Ursprüngliche Nachricht-----
Von: m-infoline.extern@m-infoline.ch [mailto:m-infoline.extern@m-infoline.ch]
Gesendet: Montag, 23. Januar 2006 15:26
An: ,
Betreff: Ticket-Nr. M-Infoline: IN_38148; M-Cumulus; Allgemein,

E
Dieses Email darf nicht an Kunden geschickt werden, es enthält
Internas! Erstellen Sie bitte ein neues Email für die Beantwortung
des Anliegens und verwenden Sie nicht die Funktionen antworten
oder weiterleiten. Danke!

Kopie an
Anliegetyp:
Auskunft / Information
Betreff:

Kontaktformular M-Infoline Deutsch
Kundenanliegen:
Liebes Migros-Team
zum Thema Datenschutz schreiben Sie auf der Homepage
http://www.m-cumulus.ch (Kontaktformular funktioniert dort leider
nicht). ..Gewissheit, dass Ihre Daten sicher verwaltet werden und
der Umgang damit vollumfänglich den gesetzlichen Anforderungen
```

```
und den weitergehenden Migros-internen Datenschutzregeln
entspricht.... da ja die gesetzlichen Anforderungen so oder so
eingehalten werden müssen und damit kein Zertifikat benötigen,
würde es mich interessieren, was die weitergehenden
Migros-internen Datenschutzregeln genau sind. Freundlich Grüsse,
Andreas Müller

Muster per Post:
Artikelnummer:
Artikelbezeichnung:
BOSS-Nummer:
Bedarfswelt:
Bedarfsbereich:
Betroffene Filiale:
Interne Kommentare:
Attachments:
Eingangsdatum:
Kundenadresse:
Herr
Andreas Müller
Postfach:
Schweiz
Sprache:
Deutsch
Anrufer-Nummer:
Email:
migros.3.user1003@spamgourmet.com
Wünscht Antwort?
True
(true = ja, false = nein)
Tel. privat:
Antwortkanal:
E-Mail
Tel. mobil:
Wann erreichbar:
Fax:
Stimmungslage:
Normal
Tel. Geschäft:
```

A.2 Bewertung

- *Daten werden nur mit einer hohen Verschlüsselung verschickt.*
  Gemeint ist wohl Verschlüsselung mit langen Schlüsseln. Ohne genauere Angaben ist dies nicht sehr aussagekräftig, aber es ist erfreulich, dass Migros überhaupt Verschlüsselung verwendet.
- *Im Direct Marketing legen wir offen, woher die Adressen kommen.*
  Erfreulich. Zumindest auf Anfrage ist dies aber wohl gesetzlich vorgeschrieben.
- *Wir betreiben keine Datenanreicherung mit externen Daten. Es wird nur das abgelegt, was bei der Nutzung der Konten anfällt.*
  Auch erfreulich.
- *Wir arbeiten nur mit Agenturen, die im SDV (Schweiz. Direct Marketing Verband) Mitglied sind.*

Gut zu wissen. Der SDV hat allerdings immerhin über 140 Mitglieder [34].

- *Wir haben nur einen kleinen Benutzerkreis, der Zugang zu den Daten hat.*
  Und zwar (Verwendung der Adressdaten, direkt kopiert von [21]): Migros-Genossenschafts-Bund, Migros-Genossenschaften, m-electronics, sportXX, DO IT + GARDEN, MICASA, OBI, Florissimail, Saisonküche, Migros-Klubschule, Migros-Freizeitzentren, Golf Parcs, Hotelplan, Eurocentres, Migrosbank, Ex Libris, Migrol.

Freundliche Grüsse
CUMULUS Marketing Services
Auch bei Mirgros scheint Datenschutz in erster Linie als Marketingproblem wahrgenommen zu werden.
Dieses Email darf nicht an Kunden geschickt werden, es enthält Internas! Erstellen Sie bitte ein neues Email für die Beantwortung des Anliegens und verwenden Sie nicht die Funktionen antworten oder weiterleiten. Danke!
Tja, oops.
Email: migros.3.user1003@spamgourmet.com
Ein Beispiel zur Verwendung von Spamgourmet. Eine Adresse xyz.N.user-1003@spamgourmet.com erlaubt es, ohne vorherige Konfiguration maximal N eMails von voriger Adresse an die echte eMail-Adresse umzuleiten. Drei eMails war in diesem Fall allerdings fast zu knapp, da vor der echten Antwort zwei automatisch generierte eMails versendet wurden.
Wünscht Antwort? True (true = ja, false = nein)
Bemerkenswert, weil diese Klassifizierung allem Anschein nach automatisch erfolgt ist.
Stimmungslage: Normal
Ein interessantes Beispiel zur automatischen Auswertung von Daten. Offenbar wird bei Migros Software eingesetzt, um z.B. besonders frustrierte oder aggresive eMails zu kennzeichnen. Es ist beruhigend zu wissen, dass diese Software meine Besorgnis um Datenschutz für normal hält :)

Literatur

[1] `http://creativecommons.org/licenses/by-nc/2.5/`
Die ≪Creative Commons Attribution-NonCommercial 2.5 License≫

[2] Die Politik der Infosphäre
Buch von Konrad Becker u.a.

[3] `http://www.admin.ch/ch/d/sr/23.html#235`
Gesetze zum Datenschutz in der systematischen Rechtssammlung des Bundes (SR 235)

[4] `http://www.admin.ch/ch/d/sr/c235_1.html`
Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)

[5] `http://www.edsb.ch/`
Eidgenössicher Datenschutzbeauftragter

[6] `http://www.datenschutz.ch`
Datenschutzbeauftragter des Kantons Zürich

[7] `http://mail.google.com`
Gmail von Google

[8] `http://www.edsb.ch/d/doku/musterbriefe/index.htm`
Musterbriefe zur Dateneinsicht

[9] http://www.admin.ch/ch/d/sr/780_1/a7.html
SR 720.1 Artikel 7

[10] http://www.admin.ch/ch/d/sr/510_10/index.html
Bundesgesetz über die Armee und die Militärverwaltung

[11] http://www.admin.ch/ch/d/sr/511_22/index.html
Verordnung über das militärische Kontrollwesen

[12] http://www.admin.ch/ch/d/sr/511_22/app1.html
Anhang zu VmK: Daten des militärischen Kontrollwesen

[13] http://www.admin.ch/ch/d/sr/c511_12.html
Verordnung über die medizinische Beurteilung der Diensttauglichkeit und der Dienstfähigkeit (VMBDD)

[14] http://www.admin.ch/ch/d/sr/511_12/app2.html
Datenbearbeitung mit MEDISA; Herkunft, Inhalt und Benutzer der Daten

[15] http://www.ccc.de
Der Chaos Computer Club

[16] http://eff.org
Electronic Freedom Foundation

[17] http://www.bigbrotherawards.ch
Big Brother Awards

[18] http://www.beobachter.ch
Beobachter (Zeitschrift)

[19] http://pages.ebay.ch/help/policies/privacy-policy.html
“Datenschutzerklärung“ von eBay

[20] http://de.wikiquote.org/wiki/Benjamin_Franklin
Wikiquote zu Benjamin Franklin

[21] http://www.m-cumulus.ch/
Homepage von Migros Cumulus

[22] http://www.m-cumulus.ch/CUMULUS_DE/Content/UeberM-CUMULUS/Datenschutz/
Migros zu Datenschutz bei Cumulus

[23] http://www.sqs.ch/index/leistungsangebot/lgpr.htm
SQS, [Not-So-]Good-Priv@cy Label

[24] http://www.gnupg.org/
Gnu Privacy Guard – freies Verschlüsselungsprogramm

[25] http://www.spamgourmet.com
Spamgourmet

[26] http://www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/
PGP Pathfinder

[27] http://de.wikipedia.org/wiki/Datamining
Wikipedia zu Datamining

[28] http://4q.squat.net/
Bert Setzer (Pseudonym) – geklonte Rabattkarte

[29] http://www2.sfdrs.ch/sf1/kassensturz/sendung/beitrag.php?beitragid=1165
Kassensturz zum Thema Adresshandel (10.1.2006)

[30] http://www.schober.ch
Schober Direktmarketing - fürs Baumsterben verantwortlich

[31] http://www.angoss.com/
Knowledge Server

[32] http://www.sas.com/products/miner/index.html
Enterprise Miner

[33] http://www.spss.com/datamine/
Scenario

[34] http://www.dmverband.ch
Schweizerischer Direktmarketingverband

[35] http://www.admin.ch/ch/d/sr/784_10/index.html
Fernmeldegesetz (SR 784.10)

[36] http://www.admin.ch/ch/d/sr/780_1/index.html
Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1)

[37] http://www.admin.ch/ch/d/sr/360_2/index.html
Verordnung über das Informationssystem der Bundeskriminalpolizei (SR 360.2)

[38] http://www.admin.ch/ch/d/sr/120_3/index.html
Verordnung über das Staatsschutz-Informations-System (SR 120.3)

[39] http://www.admin.ch/ch/d/sr/363/index.html
Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (SR 363)

[40] http://www.admin.ch/ch/d/sr/510_291/index.html
Verordnung über die Nachrichtendienste im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (SR 510.291)

[41] http://www.admin.ch/ch/d/sr/120_2/index.html
Verordnung über Massnahmen zur Wahrung der inneren Sicherheit (SR 120.2)

[42] http://www.admin.ch/ch/d/sr/510_10/a99.html
Bundesgesetz über die Armee und die Militärverwaltung Art. 99 (SR 510.10)