# Context-Aware Computing:

# Privacy Issues

Seminar Context Aware Computing
Sommersemester 2006

Institut für Informatik
Universität Zürich

**Andreas Schraffl**

**Thomas Rüegg**

# Inhaltsverzeichnis

# 1 Einführung

## 1.1 Wieso ist Context-Aware Computing eine Bedrohung für die Privatsphäre?

Durch die Allgegenwart von elektronischen Geräten, deren einfachen und effizienten Möglichkeiten zur Erhebung und Speicherung von personifizierten Daten und immer besseren und komplexeren Auswertungen verschiedener Daten kann über den Träger dieser Geräte sehr viel herausgefunden werden. Diese Daten stellen einen Einbruch in die Privatsphäre des Benutzer dar. Die Privatsphäre kann heute als ein Gut bezeichnet werden mit dem reger Handel im Gange ist. Beinahe jedes grössere Geschäft hat eine Kundenkarte kombiniert mit einem Rabattsystem. Diese Rabattsysteme dienen nicht primär zur Kundenbindung sondern zur Datenerhebung, d.h. die Geschäfte bezahlen den Kunden für seine Daten. Diese Daten beziehen sich meist auf ein Geschäft oder einen Verbund von Geschäften. Wie viel sind nun aber Daten Wert welche die Lücken zwischen diesen Geschäften füllen, wie z.B. Bewegungsdaten wie sie über das GSM-Netz erhoben werden können? Wie viel sind Reisedaten Wert welche über Ticketsysteme wie z.B. das SBB-Projekt EasyRide gewonnen werden?

## 1.2 Wert der Daten

Zwei Beispiele:

**Migros Cumulus**[1]**:** 1% Rabatt für Kunde, Migros erhält personalisierte Einkaufsdaten

**Jajah** (Kapitel 4.2).**:** Gratis telefonieren durch Rückruf. Jajah erhält Verbindungsdaten.

## 1.3 Vertrauensbasis

Die meisten Ansätze zur Sicherung der Privatsphäre basieren auf Anonymisierung (selten kommerziell Angeboten, meist mit einem Informationsverlust für den Anwender) oder Zertifikaten

1 Rabattkarte der grössten Supermarktkette in der Schweiz, mit der alle Einkäufe auf Positionsebene erfasst werden können.

und Zusicherungen über die Art der Speicherung der Daten. Das Problem bei beiden Arten ist, dass sie immer auf Vertrauen in den Anbieter basieren. Welche Anbieter sollen dies sein? Eine Staatsorganisation (Bundesamt, Kantonale Verwaltung, Polizei, ...), eine Firma (Microsoft, IBM, Google, ...)?

### 1.4 Auffälligkeit und Personifizierung

In mehreren Studien hat sich gezeigt, dass der Anwender selten Interesse hat sich über die Art der Datenverwaltung zu informieren (wenn er es denn kann). Was er hingegen passiv bemerkt sind Installationen zur Datenerhebung. Diese Installationen (Kameras, Lesegeräte, Sender) müssen für das subjektive Sicherheitsgefühl nach zwei Faktoren optimiert werden: Auffälligkeit und Personifizierung.

## 2 Vorgehen und Ziel dieser Arbeit

Wie in der Einführung dargelegt, ist der Datenschutz bei bei modernen Anwendungen insbesondere auch im Zusammenhang mit Informationen über den geographischen Aufenthaltsort einer Person komplex und der Umgang der Menschen mit diesem komplexen Thema selbst ein komplexes Gebiet an der Schnittstelle zwischen technischen und sozialen Wissenschaften sowie des Rechts und der Politik.

Da eine Untersuchung in diesem Spannungsfeld den Rahmen dieser Seminararbeit bei weitem sprengen würde, wir uns aber nicht nur auf einen einzelnen Aspekt konzentrieren sondern die ganze Breite des Themas mit den verschiedenen möglichen Zusammenhängen konzentrieren möchten, erlauben wir uns das folgende Vorgehen:

1. Wir stellen eine These auf.
2. Wir nehmen vorhandene Datenschutzprinzipien

3. Wir ziehen verschiedene Beispiele und eine Studie hinzu, um unsere These zu illustrieren und wenden auf die Prinzipien auf einige Beispiele an.

Damit wollen wir die Komplexität des Themas umreissen und einige Anregungen für Fragestellungen geben, die in Zukunft mit wissenschaftlichen Methoden untersucht werden könnten.

# 3 These und Datenschutzprinzipien

## 3.1 These

Die Beurteilung und Akzeptanz der Bekanntgabe von und anschliessenden Verarbeitung von privatsphärenrelevanten Daten hängt stark von der subjektiven Wahrnehmung der betroffenen Person ab.

## 3.2 Datenschutzprinzipien

Die Prinzipien stammen aus [1].

**Erkennbarkeit**

Datenerhebunggeräte sollten auf einen standardisierte Art erkennbar geben welche Art von Daten sie erheben. Die Personen in der Umgebung des Gerätes sollten immer die Möglichkeit haben sich über die Art der über sie erhobenen Daten zu informieren.

**Einverständnis**

Die Person muss sich explizit mit der Datenerhebung einverstanden erklären. Dies wird heute oft durch eine Unterschrift oder einen Mausklick getätigt. Dies könnte bei zukünftigen Geräten nicht mehr möglich sein, da keine Benutzereingabe vorgesehen ist. Auch müsste jeder Datentransfer bestätigt werden, was das System unnütz bar machen würde.

**Wahl**

Das ablehnen der Datenerhebung darf mit keinem Nachteil verbunden sein. Dazu müsste ein System selektiv Daten von einzelnen Personen anonymisieren können, was bei den wenigsten möglich ist.

**Anonymität | Pseudoanonymität**

Daten dürfen in anonymisierter Form erhoben werden. Die Daten dürfen nicht einfach mit einer Person verknüpft werden. Da dies personalisierte Systeme verunmöglicht wäre eine Pseudoanonymität von Vorteil, bei der eine eindeutige ID für einen Datensatz existiert, die Person aber die Möglichkeit hat diese Identität aufzugeben.

**Nähe**

Ein Datenerhebungsgerät sollte nur dann Daten erheben wenn sein Besitzer in der Nähe ist. Dies hilft, da dann weitere Personen deren Daten erhoben wird sich einer Person (die auch so beobachten könnte) bewusst sind. Dies wird am einfachsten über externe Speicher getätigt. Nur wenn der Besitzerspeicher anwesend ist kann effektiv gespeichert werden.

**Ortsgebundenheit**

Daten sollten den Erhebungsort nicht elektronisch verlassen können.

**Sicherheit**

Datensicherheit bei der Übertragung und Lagerung werden oft als Wunderheilmittel betrachtet um die Privatsphäre zu schützen. Eine sichere Datenübertragung benötigt erheblichen Rechenaufwand welcher mit einem erhöhten Strom- und Zeitgebrauch einhergeht. Unnütz für kleine mobile Geräte. Auch löst die reine Sicherheit nicht das Problem der Privatsphäre.

**Zugriff**

Datensätze sollten mit der zugehörigen Einverständniserklärung in maschinenlesbarer Form gespeichert werden. Damit sollte ein Datenauswertungssystem nur Daten auswerten zu denen es

auch eine Einverständniserklärung hat.

**Minimalität**

3 einfache Minimalitätsklauseln:

- nur Daten für einen genau definierten Zweck erheben (keine Vorratsdatenspeicherung)
- nur Daten die für den Zweck notwendig sind (nicht mehr)
- nur Daten solange behalten wie nötig

Mit diesen Prinzipien alleine kann kein vollumfänglicher Schutz der Privatsphäre sichergestellt werden. Dieser ist mit momentanen Mitteln und bei gleichzeitigem Gebrauch dieser Geräte nicht möglich. Die Datenschutzprinzipien vereinfachen es aber dem Betreiber eines Systems dem Benutzer mit einfachen Mitteln und ohne grossen Aufwand für den Benutzer die Privatsphäre zu wahren.

Über all diesen Richtlinien steht die Vertrauensbasis. Die Überprüfbarkeit dieser Richtlinien durch Einzelpersonen ist nicht möglich. Wer auch immer diese Richtlinien beachtet sollte sich durch eine externe Instanz prüfen lassen. Ob dies eine staatliche oder private Einrichtung ist, muss der Konsument entscheiden.

# 4 Beispiele

## 4.1 Locatis

Die Schweizer Firma Locatis will 2006 zusammen mit dem Mobilfunkbetreiber Orange das Lokalisierungssystem PB100 auf den Markt bringen, welches eine Lokalisation über GSM und GPS erlaubt. Rein technisch ist dies keine grosse Änderung gegenüber bereits bestehenden Systemen. Das neue an PB100 ist, dass es von einem autorisierten Suchenden aktiviert werden kann. Das System ist mit ca. 80 Gramm leicht und lässt sich einfach verstecken. Laut Locatis kann ein Suchender ein PB100 seinem Hund anbinden um ihn immer wieder zu finden. PB100 kann aber

auch für die Suche von Freunden eingesetzt worden. Da PB100 über SMS, Callcenter oder WebSeite nicht nur Koordinaten sondern auch direkt eine Adresse ausgeben kann muss nicht einmal steht der direkten Suche des Aufenthaltsortes nichts im Weg. Für zukünftige Generationen von Mobiltelefonen die GPS Positionsbestimmung bereits integriert haben soll nur noch eine Aktivierung mittels SMS benötigt sein. Ob ich ein Mobiltelefon an meinen Hund hänge oder einem Mitarbeiter mitgebe kann ich entscheiden.

**Datenschutzprinzipien:**

- **Erkennbarkeit:** Nicht vorgesehen, der Hund kann ja nichts damit anfangen.
- **Einverständnis:** Durch den Kauf des Gerätes oder SMS Bestätigung, einzelne Messungen benötigen kein Einverständnis.
- **Wahl:** Nicht vorgesehen, der Hund kann ja nicht wählen.
- **Anonymität | Pseudoanonymität:** Gegenüber Locatis ist nur der Empfänger der Auswertung bekannt. Bei Telefongeräten die über eine Telefonnummer erkannt werden ist auch der Inhaber der Telefonnummer bekannt.
- **Nähe:** Nein, da das Gerät für Ortung vorgesehen ist.
- **Ortsgebundenheit:** Liegt in den Händen des Empfängers der Daten. Da das Gerät für Ortung vorgesehen ist kann nicht weiter eingeschränkt werden.
- **Sicherheit:** Nichts bekannt.
- **Zugriff:** Keine Speicherung durch den Anbieter, Speicherung beim Empfänger offen.
- **Minimalität:** Empfänger bestimmt über die Anzahl der Daten und die Speicherdauer. Gerätebedingt werden momentan nur Positionsangaben gemessen. Ob später auch ein Audiokanal geöffnet werden kann wie dies bei ähnlichen Alarmierungssystemen möglich ist ist offen.

Generell werden die Datenschutzprinzipien nicht beachtet. Teilweise sind sie für das Anwendungsgebiet nicht sinnvoll, der Anbieter vertraut in den Kunden, dass das Gerät nur für den Hund ist.

## 4.2 Jajah

Diese US-amerikanische Firma biete gratis Telefonate an. Der Kunde gibt seine und die zu wählende Telefonnummer im Internet ein und Jajah ruft beide an und stellt eine Verbindung her. Als einfachste zu erhebende Daten sind die Verbindungsdaten hier auszumachen. Jajah erhält sämtliche Daten wer wann wen anruft. Daraus lässt sich ein soziale Netzwerk konstruieren, wer in welchen Kreisen mit wem spricht. Diese Daten dürfen laut Vertrag auch an Partnerfirmen weitergegeben werden. Ein weiterer sehr interessanter Datenbereich sind die Gespräche selbst. Moderne Spracherkennungssysteme könnten den Gesprächsinhalt wodurch ein noch besseres Kundenprofil erstellt werden kann. Da eine Telefonnummer nicht so einfach fälschbar ist wie eine Email-Adresse erhält Jajah sehr stabile Daten zu dem Kunden. Das interessanteste am Jajah Vertrag ist jedoch, dass Jajah sich vorhält, den Vertrag jederzeit zu ergänzen und dem Kunden die Verantwortung übergibt, diese Aktualisierungen zu lesen.

**Jajah End User License Agreement** [2]

4.1 By entering into this Agreement you hereby accept and incorporate by reference all terms and a condition of the Privacy Policy at the following link, as may be amended from time to time.

**Jajah Privacy Policy** [3]

Phone Calls

Among the services JAJAH offers, Users may initiate phone calls between them which are partly or fully handled via JAJAH telecom partners. Therfore any information which You may post during such phone call, including any personal information shall not be deemed private. JAJAH cannot guarantee the security of such information, that you disclose or communicate in such phone call and

you do so at your own risk.

## 4.3 SBB EasyRide

SBB EasyRide [4], [5] ist ein 1998 gestartetes Projekt welches als Ziel hatte die Benutzung des öffentlichen Verkehrs zu vereinfachen. Dies sollte mittels einer Chip-Karte welche als persönliches Billet gilt gelöst werden. Diese Chip-Karte sollte unter dem Namen EasyAccess, den schrankenlosen Zugang zu sämtlichen öffentlichen Verkehrsmittel ermöglichen. Die Infrastruktur registriert sämtliche gefahrenen Strecken. Auf deren Basis wird im Nachhinein eine Rechnung gestellt. Dies würde es jedem EasyAccess Kunden ermöglichen denselben Komfort zu haben wie es heute Besitzer eines Generalabonnements haben. Die SBB könnten Schalterpersonal und auch Zugbegleiter einsparen, da eine Billetkontrolle nur noch für die wenigen die kein EasyAccess haben nötig wäre. Das Einsparpotential beläuft sich laut SBB auf 600 Mio. CHF jährlich.

Leider ist EasyAccess auch 2006 noch ein Zukunftstraum. Laut der Projektleitung EasyRide weil die Kosten zu hoch sind, was ich aber angesichts von projektierten Installationskosten von 450 Mio. Fraglich für fraglich halte. Laut einer internen SBB Quelle seinen bei Pilotstudien die Kunden nicht zufrieden gewesen als sie einen Auszug sämtlicher gefahrener Strecken bekommen haben.

Ein weiteres Projekt im Rahmen der EasyRide Entwicklung war EasyTicket. Dies ist ebenfalls eine Chip-Karte, welche als elektronisches Ticket dient. Der Unterschied besteht in der Abrechnungsart. Während bei EasyAccess der Kunde Nachträglich eine Liste der gefahrenen Strecken erhält muss man bei EasyTicket die Strecken vorher kaufen. Der Vorteil für den Kunden ist, dass er nicht jedes mal ein neues Papierticket bekommt, sondern alles auf einer Chip-Karte hat. Der Vorteil für die Anbieter sind eine einfachere Abrechnung und fairere Verteilung der Einnahmen auf die verschiedenen beteiligten des öffentlichen Verkehrs.

Leider geht der Komfort für den Reisenden dabei verloren. Dafür müssen die Daten nicht personalisiert gespeichert werden, sondern können in anonymisierter Form vorliegen. Dies war

auch bei den Mobiltelefondaten der Fall bis sich die Strafverfolgung für die Daten interessierte. Das heute die Positionsangaben von den Mobilfunkbetreibern für 6 Monate personalisiert gespeichert werden müssen ist fast niemandem bewusst.

## 4.4 Ortung von Mobiltelefonen

### Die Zeitungsmeldung

Am Sonntag 28. September 1997 war in der SonntagsZeitung folgendes zu lesen: „Innere Sicherheit ist nicht nur Sache der Polizei – Wovon Kriminalisten und Staatsschützer jahrelang geträumt haben, ist Wirklichkeit geworden. Auf Missetäter lässt sich – der Mobiltelefonie sei Dank – in der Schweis permanent zurückgreifen. Im Geheimen wurde ein enges Überwachungsnetz installiert. Auch unbescholtene Natelbenutzer[2] werden damit auf Schritt und Tritt verfolgt – für den Fall, dass einer den Pfad der Tugend verlässt...“ Die Zeitung wurde angeblich sogar gebeten, den Artikel und die Existenz dieser Ortungsmöglichkeit nicht zu publizieren[6]. Obschon jedermann bei genauerem Nachdenken eigentlich klar werden müsste, dass ein Mobilfunksystem mit mehreren Antennen eine Instanz braucht, die von jedem Teilnehmer weiss, im Umkreis welcher Antenne er sich befindet und man sich weiter bewusst ist, dass einmal vorhanden Daten auch ausgewertet werden können, löste diese Medienmitteilung ein grosses Echo aus.

### Die Untersuchung

Die Beunruhigung in der Öffentlichkeit führte dazu, dass sich der Eidgenössische Datenschutzbeauftragte[3] mit einer Untersuchung des Falles an nahm und am 6. Juli 1998 die Medien über die Ergebnisse der Untersuchung informierte [7]. Er fand heraus, dass die Daten nur auf der Ebene von 30 regionalen Gebieten gespeichert werden und dass die Bearbeitung der Daten

2 Natel®: Nationales Autotelefon, Marke der Swisscom, Nachfolger des ehemals staatlichen Telekommuniktationsteils der Schweizerischen Post. Zu diesem Zeitpunkt gabe es nur die Swisscom als Anbieter von Mobilfunkdiensten, weshalb Natel noch heute in der Schweiz ein gebräuchlicher Begriff für ein Mobiltelefon ist.

3 Der Eidg. Datenschutzbeauftragte heisst neu Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). Seine Website ist unter http://www.edoeb.admin.ch zugänglich.

im Einklang mit dem Datenschutzgesetz (DSG) [8] von 1992 geschehen. Allerdings machte er bei der Aufbewahrungsfrist einen Vorbehalt: diese dürfe die in der Fernmeldeverordnung vorgesehene Frist von 6 Monaten nicht übersteigen. Zudem hielt er fest, dass die Zusammenarbeit während der Untersuchung mit den involvierten Stellen meistens gut verlief, was allerdings auch darauf hinweist, dass es auch Probleme gab. Es ist wenig erstaunlich, dass die weniger gute Zusammenarbeit die heiklen Bereiche betrifft, namentlich die Generalsekretäre der Departemente für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und für Justiz und Polizei (EJPD). Auf jeden Fall wolle er die Verwendung dieser Daten weiter überwachen und er verlangt, dass die Datensammlungen wie im DSG vorgesehen, bei ihm registriert werden müssen. Ein interessantes Detail stellt die Meinung dar, dass es keinen Grund für die Registrierung von Kunden von Prepay Handys (Natel Easy) gäbe.

**Heutige Situation**

Gemäss heutiger Rechtslage, definiert im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) [9] aus dem Jahre 2000 und der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) [10] aus dem Jahre 2001 müssen die Anbieter bei dringendem Verdacht auf Verübung oder Beteiligung an abschliessend aufgezählten schweren strafbaren Handlungen, Versagen sämtlicher anderer Ermittlungsmethoden und einer Genehmigung durch ein Organ der Justiz mit den Ermittlungsbehörden zusammenarbeiten. Dazu müssen sie bis 6 Monate rückwirkend sämtliche Verkehrs- und Rechnungsdaten liefern können, die explizit auch den Antenntenstandort und die Hauptabstrahlrichtung beinhalten. Zudem müssen die Dienstanbieter Verschlüsselungen entfernen und sicherstellen, dass die überwachte Person die Überwachung nicht bemerkt. Neu ist es auch nicht mehr möglich, Prepay SIM Karten zu erwerben, ohne sich zu registrieren, da solch unregistrierte Karten eine perfekte Kommunikationsmöglichkeit für Terroristen und andere Verbrecher darstellen.

Konkret bedeutet dies, dass der Aufenthaltsort jeder Person, die ein Mobiltelefon auf sich trägt von

den Strafverfolgungsbehörden jederzeit und auch bis 6 Monate im Nachhinein festgestellt werden kann. Gemäss Gesetz gibt es keine Grundlage, die Daten über diese 6 Monate hinaus aufzubewahren, allerdings lässt sich dies nur schwer überprüfen. Die meisten Leute, die täglich ein Mobiltelefon auf sich tragen, dürften sich dieser Tatsache bewusst sein. Eine kurze informelle Umfrage fördert auf jeden Fall kein Bewusstsein zu diesem Thema zu Tage.

## 4.5 Studie: Privacy and Rationality in Individual Decision Making

Alessandro Acquisti von der Carnegie Mellon University (CMU) und Jens Grossklag von der University of California, Berkley haben im Jahre 2004 an der CMU eine Studie zu Rationalität bei Entscheidungen zum Thema Privatsphäre durchgeführt [11]. Die Studie wird in diesem Unterkapitel vorgestellt und die wichtigsten Ergebnisse werden besprochen.

**Einordnung**

In der Präsentation der Studie unterscheiden die Autoren die seit langem auf Entscheidungsprobleme in Fragen rund um die Privatsphäre angewendeten ökonomischen Theorien von ihrem Ansatz, wonach sich Individuen bei solchen Entscheidungen nicht streng rational Verhalten. Bei ersteren geht es darum, dass bei jeder Entscheidung über die Preisgabe von persönlichen Daten eine rationale Entscheidung aufgrund der zu erwartenden Kosten und des zu erwartenden Nutzens gefällt wird. Eine solch rationale Entscheidung unterliegt aber diversen, teilweise impliziten Voraussetzungen.

Erstens ist die Information zum Zeitpunkt der Entscheidung meistens unvollständig. So können Daten zum Beispiel später ergänzt, weitergegeben und/oder kombiniert werden, was die Kosten massiv verändern kann. Oft ist die Information auch asymmetrisch verteilt und der Empfänger der Daten weiss wesentlich besser über die Nutzung der Daten Bescheid als derjenige, der die Daten zur Verfügung stellt. Auch auf Seite der Nutzen ist die unvollständige Information ein Problem. Die Produkte sind häufig komplex und verschachtelt. Risiko und Unsicherheit prägen die

Entscheidungssituation.

Zweitens ist die Anzahl der Faktoren, die die effektiven Kosten bzw. den Nutzen bestimmen, sehr gross. Selbst wenn ein Individuum Zugang zu allen Informationen hätte, wäre es kaum in der Lage, diese auch alle zu verarbeiten. Dies führt zu Abweichungen vom rationalen Entscheidungsprozess.

Drittens, falls die Information vollständig und die Kapazität zur Berücksichtigung aller Faktoren gegeben wäre, gibt es immer noch Gründe, wieso ein Individuum von der rationalen Entscheidung abweicht. So zitieren die Autoren Experimente, die zeigen, dass Verlust stärker negativ wahrgenommen wird als Gewinn in gleicher Höhe positiv bewertet wird. Auch gibt es Hinweise, dass ein sofortiger Gewinn bevorzugt wird, selbst wenn die Kosten grösser sind. Eine solche Situation ist zum Beispiel bei den diversen Kundenkarten gegeben, die innert nützlicher Frist Gewinn in Form von Sonderangeboten versprechen und deren Kosten in Form von Nachteilen aufgrund von Persönlichkeitsprofilen aus den gewonnenen Daten später beträchtlich sein könnten.

Trotz dieser Kritikpunkten sind die ökonomischen Theorien weit verbreitet. Dürfte sein, dass sie sich gut verkaufen lassen. Wenn ein Anbieter davon ausgeht, dass der Kunde rational entscheidet, muss er nur einige Informationen bereitstellen und dem Kunden eine Wahlmöglichkeit geben und hat somit dem Schutz der Privatsphäre seiner Kunden genüge getan. Ein anderer Grund dürfte sein, dass politische Diskussionen über die Rolle des Staates in der Diskussion um den Schutz der Privatsphäre wesentlich weniger kontrovers geführt werden können (vgl. Kapitel 5).

**Basis**

Für die Studie wurden Personen an der CMU zum online Thema Präferenzen bei eCommerce befragt, um Selbstselektion von an Datenschutz interessierten Personen zu verhindern. Es haben 119 Personen teilgenommen, wobei das Alter zwischen 19 und 55 Jahren lag, der Durchschnitt betrug 24 Jahre. Mehr als die Hälfte war arbeitete  Voll- oder Teilzeit oder war arbeitslos, auch wenn die Studierenden mit 41.3 % die grösste Gruppe stellte. Alle Teilnehmer hatten ein

abgeschlossenes Studium oder waren am studieren. Das Sample ist also sicher nicht repräsentativ. Das Haushaltseinkommen ist verhältnismässig gering und die meisten benutzen häufig Computer, sowohl am Arbeitsplatz wie auch zuhause.

**Einstellung zur Privatsphäre**

Ein Grossteil der Studienteilnehmer äusserten starke oder mittlere generelle Bedenken zum Thema Privatsphäre (vgl. Tbl. 1). Über 70 % waren der Meinung, dass der Datenschutz in der heutigen Gesellschaft nicht genügt. Bei Fragen zur Einordnung der Wichtigkeit von Datenschutz zeigte sich, das Bildungspolitik zwar wichtiger, aber Terrorgefahr, Umweltpolitik und gleichgeschlechtliche Heirat weniger wichtig eingeschätzt wurden. Es zeigte sich eine Korrelation zwischen dem Einkommen und den Bedenken zum Datenschutz; diejenigen mit tiefen Einkommen waren etwas weniger besorgt als diejenigen mit höherem Einkommen. Tabelle 1 zeigt, dass Daten über die Identität (Emailadresse, Name etc.) grössere Bedenken erzeugen als von der Identität losgelöste Profildaten (wie Alter, Beruf, politisches Profil etc.)

| Grad der Bedenken | Generelle Bedenken | Daten über online Identität | Daten über offline Identität | Daten über privates Profil | Daten über berufliches Profil | Daten über sexuelle und politische Identität |
|---|---|---|---|---|---|---|
| hoch | 53.7 % | 39.6 % | 25.2 % | 0.9 % | 11.9 % | 12.1 % |
| mittel | 35.5 % | 48.3 % | 41.2 % | 16.85 % | 50.8 % | 25.8 % |
| tief | 10.7 % | 12.1 % | 33.6 % | 82.3 % | 37.3 % | 62.1 % |

*Tabelle 1: Einstellungen zur Privatsphäre[11]*

Eine Clusteranalyse ergab vier Gruppen, eine mit hohen Bedenken in allen Bereichen, zwei mit mittleren Bedenken, je im Bereich der online und offline Identität und eine letzte Gruppe mit wenigen Bedenken in allen Bereichen. Interessanterweise zeigten über 40% derjenigen, die Datenschutz als sehr wichtig angaben, nur mittlere bis wenige Bedenken um ihre Privatsphäre an. Eine Mehrheit sieht Datenschutz auch im Zusammenhang mit persönlicher Würde und der Freiheit, sich zu Entwickeln. Nur eine Minderheit stimmt mit Datenschutz als der Möglichkeit, seinem Fluss

von persönlicher Information einen Geldwert zuzuordnen.

Es zeigt sich also, das die Einstellung zur Privatsphäre und dem Datenschutz von diversen Faktoren abhängt.

**Datenschutzbezogenes Verhalten**

Die Studie untersucht bei der Befragung zwei Formen von Verhalten: Die Übernahme von Datenschutzstrategien und die Bekanntgabe von persönlichen Informationen. Zu ersteren wurde der Gebrauch von verschiedenen Technologien untersucht. Die Mehrheit macht keinen Gebrauch von Emailverschlüsselung, Alarmen bei Überschreitung bestimmter Limiten bei der Belastung der Kreditkarte oder der Sperrung des Telefonbucheintrags. Trotzdem zeigt sich bei einer Kumulation über alle Massnahmen, dass 75 % irgendeine Aktion zum Schutz ihrer Privatsphäre unternehmen. Dies zeigt, dass das Verhalten keineswegs konstant ist und von vielen Faktoren beeinflusst wird.

Zum Verhalten bei der Bekanntgabe von persönlichen Informationen wurden verschiedene Fragen zu verschiedenen Kontexten gestellt. So gaben zum Beispiel knapp über 20 % an, schon einmal ihre Social Security Number und knapp 30 % ihre Telefonnummer für Vergünstigungen an. Eine Clusteranalyse ergab zwei Gruppen, eine von knapp zwei Dritteln, die mehr Daten preis gaben und ein höheres Risiko in Kauf nahmen als die andere Gruppe von etwas mehr als einem Drittel.

Interessant ist ein Vergleich zwischen Einstellung und Verhalten von Personen. Wenn, wie beschrieben von komplexen psychologischen Einflüssen ausgegangen wird, muss dabei darauf geachtet werden, dass sowohl die Aussagen zur Einstellung wie auch zum Verhalten im selben Kontext gemacht werden. Auch unter Beachtung des Kontextes fanden sich eklatante Diskrepanzen zwischen Einstellung und Verhalten von Individuen. So gaben über 80 % der Teilnehmer, die grosse Bedenken betreffend ihrer offline Identität haben an, mindestens eine Rabattkarte für Kunden zu besitzen. Nur ein Viertel derjenigen, die bei der Freitextfrage nach ihren Bedenken zum Datenschutz Angst vor Kreditkartenbetrug angaben, machten Gebrauch von Alarmmechanismen bei

ihrer Kreditkartenabrechnung und über 60 % derjenigen die für den Einsatz von Technologien zum Schutz der Privatsphäre sind haben noch nie Emailverschlüsselung und 50 % noch nie einen Aktenvernichter für sensitive Unterlagen verwendet.

**Analyse**

Die gefundenen Diskrepanzen deuten nicht auf irrationales oder sorgloses Verhalten hin. Die Individuen treffen Entscheidungen, die dem Schutz der Privatsphäre Rechnung tragen und auf der vorhandenen Information und den Kosten und Nutzen basieren, aber eben auch noch von diversen anderen Faktoren wie fehlender Information, begrenzter Rationalität und systematischen psychologischen Abweichungen von der Rationalität beeinflusst werden.

Viele Individuen verfügen nur über unvollständige Informationen. Eine Ergänzungsstudie hat gezeigt, dass die meisten Individuen das Risiko eines Datenmissbrauchs unterschätzen. So haben nahezu zwei Drittel der Probanden die Gefahr der Verkettung von verschiedenen Informationen unterschätzt, als sie die Wahrscheinlichkeit, einen Bürger in den USA anhand seines Geschlechts, Geburtsdatums und seiner Postleitzahl zu identifizieren auf unter 50 % geschätzt. Der wahre Wert liegt aber gemäss Berechnungen der CMU bei 87 %. Auch hatten viele Teilnehmer nur bescheidene Kenntnisse der existierenden Technologien oder der Rechtslage zum Schutz der Privatsphäre.

Wie schon erwähnt, ist die Kapazität des Menschen für das Sammeln und anschliessende Bewerten von Information im Hinblick auf eine Entscheidung begrenzt. So zeigte sich in der Befragung, das weniger als 50 % der Individuen mit grossen Bedenken zum Thema Datenschutz informiert waren über Richtlinien ihres Arbeitgebers betreffend die Überwachung am Arbeitsplatz. Ein Hinweis auf ein vereinfachtes mentales Modell liefert der Befund, das ein Drittel der Teilnehmer bei der Frage, wer bei einer Bestellung über Internet mit Kreditkartenzahlung alles Einblick in die Daten der Transaktion erhalte, neben sich selbst und dem Händler die Bank bzw. Kreditkartenfirma zu nennen vergassen. Wenn man sie darauf aufmerksam machte wurde sofort klar, dass sie das prinzipiell schon wussten, aber zum Zeitpunkt der Befragung gerade nicht im Kopf hatten. Ebenso

wahrscheinlich ist, dass solche Lücken zwischen grundsätzlichem Wissen und momentanen Bewusstsein auch bei realen täglichen Entscheidungssituationen auftreten.

Bei den systematischen psychologischen Abweichungen von der Realität wird in der Präsentation der Studie auf das Phänomen der zeitinkonsistenten Diskontierung aufmerksam gemacht, obwohl in der Studie selber keine direkten Hinweise darauf gefunden werden konnten. Bei diesem Phänomen geht es darum, dass Individuen heutige Gewinne gegenüber späteren Verlusten im vergleich zur normalen Diskontierung zu hoch bewerten. Es könnte also sein, dass die Einsparungen durch das nicht Anwenden von Technologien zum Schutz der Privatsphäre im Vergleich zum später eintretenden Schaden zu hoch gewichtet wird.

# 5 Schlussfolgerung

Die Beispiele und die Studie illustrieren, dass die Wahrnehmung von Datenschutzproblemen durch die betroffenen von vielen komplexen Faktoren abhängt und die Entscheidungen die auf Basis dieser Wahrnehmung gefällt wird, längerfristig dem Schutz der Privatsphäre nicht immer dienlich ist.

Das Modell der Rationalen Entscheidung kann zwar mit diesen Beispielen und der Studie nicht widerlegt werden, es kommen aber viele Hinweise zusammen, die darauf hindeuten, dass es nicht das beste Modell zur Beschreibung von solchen Entscheiden ist. Ein häufiger Faktor ist die unvollständige Information und die betrifft in den meisten Beispielen und in der Studie eigentlich immer breit verfügbare und etablierte Anwendungen. Im Hinblick Anwendungen aus dem Gebiet von context aware und ubiquitous Computing, die völlig neue Dimensionen eröffnen, scheint es nicht adäquat zu sein, dem Benutzer einfach eine kryptische Datenschutzerklärung zu präsentieren, sie zum Bestandteil eines Vertrages zu machen und zu erwarten, das Thema Datenschutz und Privatsphäre sei damit gelöst.

Genauso, wie die Welt der Computerwissenschaft über ihre Grenzen hinaus nach Möglichkeiten

sucht, beispielsweise Context Information zu erheben um wirkliches context aware Computing zu bieten, bietet es sich auch an, andere Disziplinen als bisher zur Erforschung des Umgangs mit neuen Herausforderungen im Bereich des Datenschutzes bei zuziehen. Viele der hier genannten Faktoren, die die Wahrnehmung der Bedrohung der Privatsphäre betreffen, lassen sich nicht einfach nur mit technisch ausgefeilten Lösungen beeinflussen. Sollte dies auch nur partiell eines Tages trotzdem gelingen, dann sicher nur, wenn die Phänomene vorher besser verstanden wurden.

Wir regen daher an, den in der Studie gefundenen Hinweise, die gegen das rationale ökonomische Entscheidungsmodell sprechen weiter zu verfolgen. Auch die Ansätze zur Erklärung dieser Hinweise wie der Einfluss der unvollständigen Information aber auch der beschränkten Rationalität und der zeitinkonsistenten Diskontierung weiter zu verfolgen. Dazu braucht es eine interdisziplinäre Zusammenarbeit mit den Sozialwissenschaften und auch mit dem Gebiet der verhaltensorientierten Wirtschaftswissenschaften. Wie in der Studie erwähnt gibt es ja bereits diverse Arbeiten zu den Phänomenen, die sich allerdings nicht auf dem Gebiet der Privatsphäre und des Datenschutzes bewegen. Hier öffnet sich ein weites Feld für weitere Experimente.

Daneben sollten die bereits gefundenen Resultate aber auch direkt in die Forschungsarbeiten zu neuen Anwendungen auf dem Gebiet des context aware und ubiquitous Computing einfliessen. Durch neue Mensch-Maschinen-Schnittstellen dürften sich auch neue Wege zur Vermittlung von Informationen über die Privatsphäre und auch zum Bewusstsein von Datenschutzproblemen finden lassen.

Eine wichtige Frage stellt sich bei der Motivation zukünftiger Hersteller von neuen Anwendungen, das Thema Datenschutz überhaupt zu beachten. Falls die sich die Richtung, in die die hier dargestellten Hinweise und Theorien deuten, als zutreffend erweist, könnte man die gewonnenen Erkenntnisse natürlich auch dazu missbrauchen, Datenschutzprobleme vor den zukünftigen Benutzern zu verschleiern. Diese Diskussion betrifft alle, auch wenn sie weit weg von den technischen Wissenschaften ist. Zum einen ergeben sich hieraus interessante Fragestellungen für

Juristen auf dem Gebiet der Gesetzgebung zum Thema Datenschutz, v. a. ist es aber eine Diskussion, der sich die Politik und die ganze Gesellschaft stellen muss. So kann man sich zum Beispiel fragen, ob es aufgrund der Tendenz zu nicht rationalen Entscheidungen bei Fragen zum Datenschutz nicht eine Aufgabe des Staates wäre, die Bürger durch Gesetze und entsprechende Kontrolle vor Missbrauch zu schützen. Oder braucht es einfach ein kleveres Modell, dass es den den Individuen erlaubt, trotz allem rationale Entscheidungen zu fällen?

# Literaturverzeichnis


1: M. Langheinrich, Privacy by Design - Principles of Privycy-Aware Ubiquitous Systems, 2001.

2: JAJAH Inc., JAJAH End User License Agreement, 2006, http://www.jajah.com/info/about/eula.aspx

3: JAJAH Inc., JAJAH Privacy Policy, 2006, http://www.jajah.com/info/about/privacy.aspx

4: A. Ott-Wirz, "easy ride"! Orwell lässt Grüssen,Winterthur , 1999.

5: Th. Gyger OD, Easyride: Active Transponders for a Fare Collection System, 2001.

6: Martin Stoll, "Innere Sicherheit ist nicht nur Sache der Polizei", Sonntagszeitung,28. Dezember 1997,TA-Media AG.

7: Eidg. Datenschutzbeauftragter, Bericht des Eidg. Datenschutzbeauftragten über die Bearbeitung von Personendaten durch die Swisscom AG im Mobiltelefonbereich (Natel-Netz) Zusammenfassung, 2006, http://www.edoeb.admin.ch/dokumentation/00438/00465/00863/00865/index.html?lang=de

8: Schweizerische Eidgenossenschaft, Bundesgesetz über den Datenschutz, 2006, http://www.admin.ch/ch/d/sr/2/235.1.de.pdf

9: Schweizerische Eidgenossenschaft, Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), , http://www.admin.ch/ch/d/sr/7/780.1.de.pdf

10: Schweizerische Eidgenossenschaft, Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, , http://www.admin.ch/ch/d/sr/7/780.11.de.pdf

11: A. Aquisti, J. Grossklag, "Economics of Information Security: Privacy and Rationality in Individual Decsision Making", *IEEE Security & Privacy*, vol. 3, no. 1, 2005, pp. 26 -33.