



Privacy Issues

07/03/06

Thomas Rüegg, Andreas Schrafl

Übersicht

- These
- Datenschutzprinzipien
- Locatis PB100
- SBB EasyRide
- Verbindungsdaten Mobiltelefone
- Studie

These

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

Datenschutzprinzipien

(nach Marc Langheinrich)

- Erkennbarkeit
- Einverständnis & Wahl
- Anonymität | Pseudoanonymität
- Nähe & Ortsgebundenheit
- Sicherheit
- Minimalität

Erkennbarkeit

- Benutzer ist informiert, dass Daten gemessen werden.
- Nicht nur Experten, jeder sollte die Daten, die gemessen werden, kennen.

Einverständnis & Wahl

- Benutzer hat ausdrücklich in die Messung eingewilligt
- Es entsteht kein Nachteil für einen Benutzer der nicht in die Messung einwilligt

Anonymität | Pseudoanonymität

- Benutzer kann anonym bleiben (in der Masse nicht eindeutig identifizierbar)
 - Wenn keine Einverständniserklärung existiert
- Pseudoanonymität über ID
 - Dienst kann individualisiert werden
 - Benutzer kann ohne Aufwand eine neue ID haben
 - www.mailinator.com

Nähe & Ortsgebundenheit

- Daten können nur erhoben werden wenn der Geräteinhaber in der Nähe ist
 - Inhaber - ID
 - Datenspeicherung nur auf wearable device
- Daten bleiben am Ort der Messung
 - Daten lagern in einem ortspezifischen Speicher
 - Daten werden nicht auf anderen Speicher kopiert

Sicherheit

- Datensicherheit ist auf längere Zeit nicht realisierbar
 - Rechenkraft steigt weiterhin an
 - Beschränkte Rechenkraft der mobilen Geräte
- Sicherheit ist kein Allheilmittel
- Allheilmittel wird nicht benötigt wenn oben genannte Prinzipien eingehalten werden

Minimalität

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

Locatis: PB100

- Lokalisation über GSM oder GPS
- Netzbetreiber: Orange
- Gerät:
 - PB100
 - Mobiltelefon
- Aktivierung mittels SMS-Bestätigung

Nutzen

- Hunde wiederfinden



Weitere Möglichkeiten

- Personen lokalisieren
- Fahrzeuge lokalisieren

Weiterentwicklung

- Nächste Generation nur Natel
- Verkleinerung des Gerätes

Locatis PB100

- **Erkennbarkeit**
 - momentan: Gerät, Natel?
- **Einverständnis & Wahl**
 - momentan: Gerät, später: SMS, temporär ausschaltbar?
- **Anonymität | Pseudoanonymität**
 - Nein
- **Nähe & Ortsgebundenheit**
 - Nein
- **Sicherheit**
 - Ja, Möglichkeiten beschränkt
- **Minimalität**
 - Ja, wenn keine Daten gespeichert werden, Speicherung durch Benutzer?

SBB: EasyRide

- Elektronisches Ticket
- Projekt seit: 1998
- Erste Machbarkeitsstudien: 1999
- Markteinführung geplant:
 - Ursprünglich: 2004
 - Momentan: 2006
 - Realistisch: 2008

SBB: EasyRide: EasyAccess

- Chip-Karte
- Schrankenloser Zugang zum öffentlichen Verkehr
- GA-Komfort für alle
- Nachträgliche Abrechnung
- Gerechtere Verteilung des Ertrags
- Weniger Schalterpersonal

SBB: EasyRide: EasyAccess

- Abrechnung erfordert Datenspeicherung sämtlicher gefahrener Strecken
- Projekt auf Eis gelegt: Kosten zu hoch
 - Installation:
450 Mio. CHF
 - Einsparungen Schalterpersonal:
600 Mio. CHF / Jahr
- Projekt auf Eis gelegt laut SBB CIO Philip Spiegel:
Datenschutzbedenken der Reisenden

SBB: EasyRide: EasyTicket

- Chip-Karte
- Elektronisches Billet wird auf Karte geladen
- Keine Papierbillets
- Gerechtere Verteilung des Ertrags
- Vorauszahlung

SBB: EasyRide: EasyTicket

- Abrechnung erfolgt vor der Fahrt
- Fahrtdaten müssen nicht gespeichert werden
- Verteilung des Ertrags erfordert Datenspeicherung
- Anonymisierbar

SBB: EasyRide: Unterschiede

Sichtbarkeit für den Kunden:

- EasyAccess: Konsument bekommt Auszug seiner Fahrten: direkt ersichtlich
- EasyTicket: Konsument vertraut der SBB: nicht direkt ersichtlich

Handy: Die Enthüllung

„Innere Sicherheit ist nicht nur Sache der Polizei

Wovon Kriminalisten und Staatschützer jahrelang geträumt haben, ist Wirklichkeit geworden. Auf Missetäter lässt sich – der Mobiltelefonie sei Dank – in der Schweiz permanent zurückgreifen. Im geheimen wurde ein enges Überwachungsnetz installiert. Auch unbescholtene Natelbenutzer werden damit auf Schritt und Tritt verfolgt – für den Fall, dass einer den Pfad der Tugend verlässt...“

SonntagsZeitung 28. Dezember 1997

Handy: Die Untersuchung

Bericht des Eidg. Datenschutzbeauftragten

6. Juli 1998

- 30 regionale Gebiete
- Besuch Swisscom Mobile Center und DAB (UVEK)
- Meist gute Zusammenarbeit

Fazit

- DSG konform ausser Aufbewahrung (6. Monate FMG)
- Weitere Überwachung
- Keine Rechtsgrundlage für Beschränkung des Auskunftrechts
- Keine Notwendigkeit zur Registrierung von Natel Easy
- Datensammlungen müssen angemeldet werden
- Zusammenarbeit muss von allen unterstützt werden

Handy: Situation heute

- Die Überwachung ist heute kein allgemeines Thema und das Bewusstsein ist gering.
- **Gesetzliche Lage** (BÜPF und VÜPF 2002):
 - Abschliessende Aufzählung der Straftaten
 - Verkehrs- und Rechnungsdaten auch 6 Monate rückwirkend
 - Standort und Hauptstrahlrichtung der Antenne
 - Zufallsfunde nach Genehmigung verwertbar, immer bei Fahndung
 - Dienstanbieter muss Verschlüsselung entfernen
 - Überwachte Person darf nichts merken
 - Prepaidkunden müssen erfasst werden

Studie: Einordnung

- **Standardmodell: Kosten/Nutzen**
 - Lässt sich gut verkaufen
 - Ist geläufig und wird auch sonst oft verwendet
 - Setzt vollständige Information und Rationalität voraus
 - Überlässt Verantwortung dem Kunden und Massnahmen dem Markt
- **Kritik**
 - Voraussetzungen sind oft nicht gegeben
 - Theorie erklärt Verhalten häufig nicht
 - Ergebnisse der Studie

Studie: Basis

- Carnegie Mellon University
- 119 Teilnehmer
- Alter 19 bis 55, Durchschnitt 24
- Alle studiert, 41.3 % Studierende

Studie: Einstellung

- Datenschutz ungenügend (>70 %)
- Datenschutz ist wichtig
 - Weniger wichtig als Bildungs- und Wirtschaftspolitik
 - Wichtiger als Terrorgefahr, Umweltpolitik und gleichgeschlechtliche Heirat
- 4 Cluster
 - Grosse Bedenken in allen Bereichen
 - Bedenken zur Online Identität
 - Bedenken zur Offline Identität
- Mehrheit sieht Datenschutz auch im Zusammenhang mit Würde und persönlicher Entwicklung

Studie: Verhalten

- Mehrheit macht kein Gebrauch von
 - Email Verschlüsselung
 - Kreditkartenalarm
 - Sperrung der Telefonnummer im Telefonbuch
- Aber: Mehrheit benutzt wenigstens eine Massnahme
 - Falsche Informationen in Formularen
 - Eingabeprozesse abbrechen
- 87.5% mit grossen Bedenken nehmen an Kundenkartenprogramm Teil

Studie: Analyse

- Verhalten stark von den Umständen abhängig und nicht konsistent
- Beschränkte Rationalität
- Problem der zeitinkonsistenten Diskontierung

Fazit

- Rationales Modell trifft nicht zu
- Information und v. a. Bewusstsein der betroffenen ist sehr wichtig
- Grosse Asymmetrie zwischen Möglichkeiten des Anbieters und der Wahrnehmung des Kunden

Fragen?

Vielen Dank fürs Wachbleiben