Karlsruher Institut für Technologie

Datenschutz und Privatheit in vernetzten Informationssystemen

Kapitel 1: Einführung

Erik Buchmann (buchmann@kit.edu)

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

Agenda für heute

- Vorstellung des Dozenten
- Gliederung der Vorlesung
- Allgemeine Einführung in die Datenschutzproblematik

Zum Dozenten

- Dr.-Ing. Erik Buchmann
  - Studium und Promotion an der Universität Magdeburg
  - seit 2006 am IPD, Lehrstuhl Prof. Böhm
  - seit 2007 Leiter der Nachwuchsgruppe *„Privacy Awareness in Information Systems and its Implications on Society“*

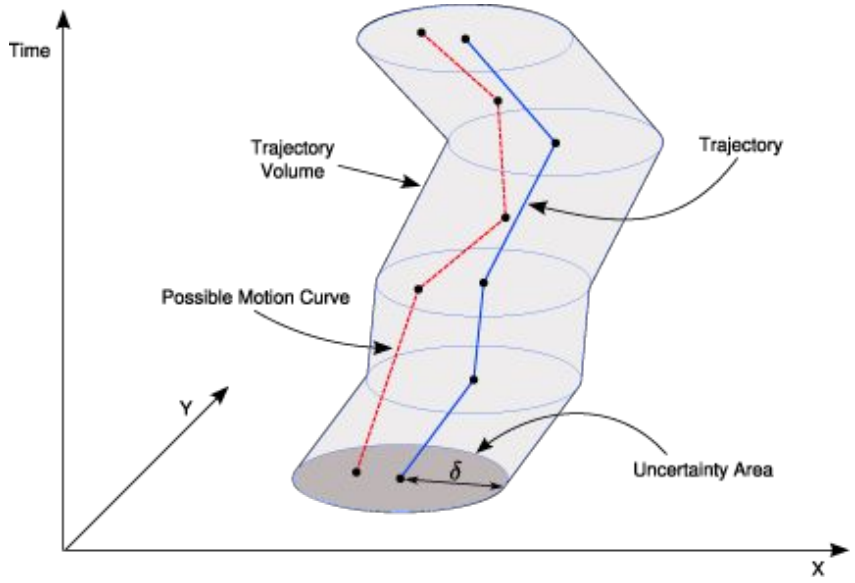
- Interessensfelder
  - Verteiltes Datenmanagement für Sensornetze und Smart Grid
  - Anfragen an unzuverlässige Sensordaten mit Orts- und Zeitbezug
  - Datenschutz und Informationelle Selbstbestimmung

- Kontakt
  - buchmann@kit.edu

Aktuelle Forschungsschwerpunkte (1/3)

- Räumlich-Zeitliche Anfragen auf ungenaue Daten
  - Sensornetze, GPS oder WLAN-Triangulierung liefern ungenaue Daten
  - Beispielanfrage: „Wieviele Objekte befanden sich vor 10 Minuten in einer bestimmten Region?“

- Forschungsfragen
  - Semantik von Ergebnissen → weg von „Best Effort“
  - Anfrageergebnisse mit Garantien auf ungenaue Datenbestände

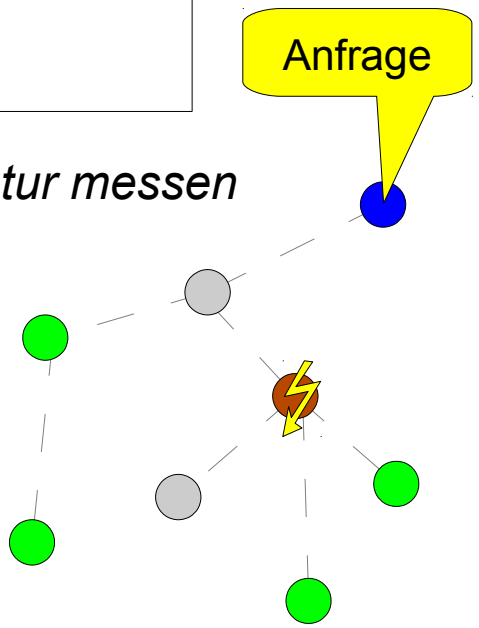


Aktuelle Forschungsschwerpunkte (2/3)

- Defektlokalisierung in Sensornetzen
  - Beispielanfrage: korreliert die Luftfeuchte (h) und der Luftdruck (p) im Habitat mit der Temperatur (t)?

```
SELECT AVG(|A.h - B.h|), AVG(|A.p - B.p|)
FROM Sensors A, Sensors B
WHERE |A.t - B.t| < 0.2
```

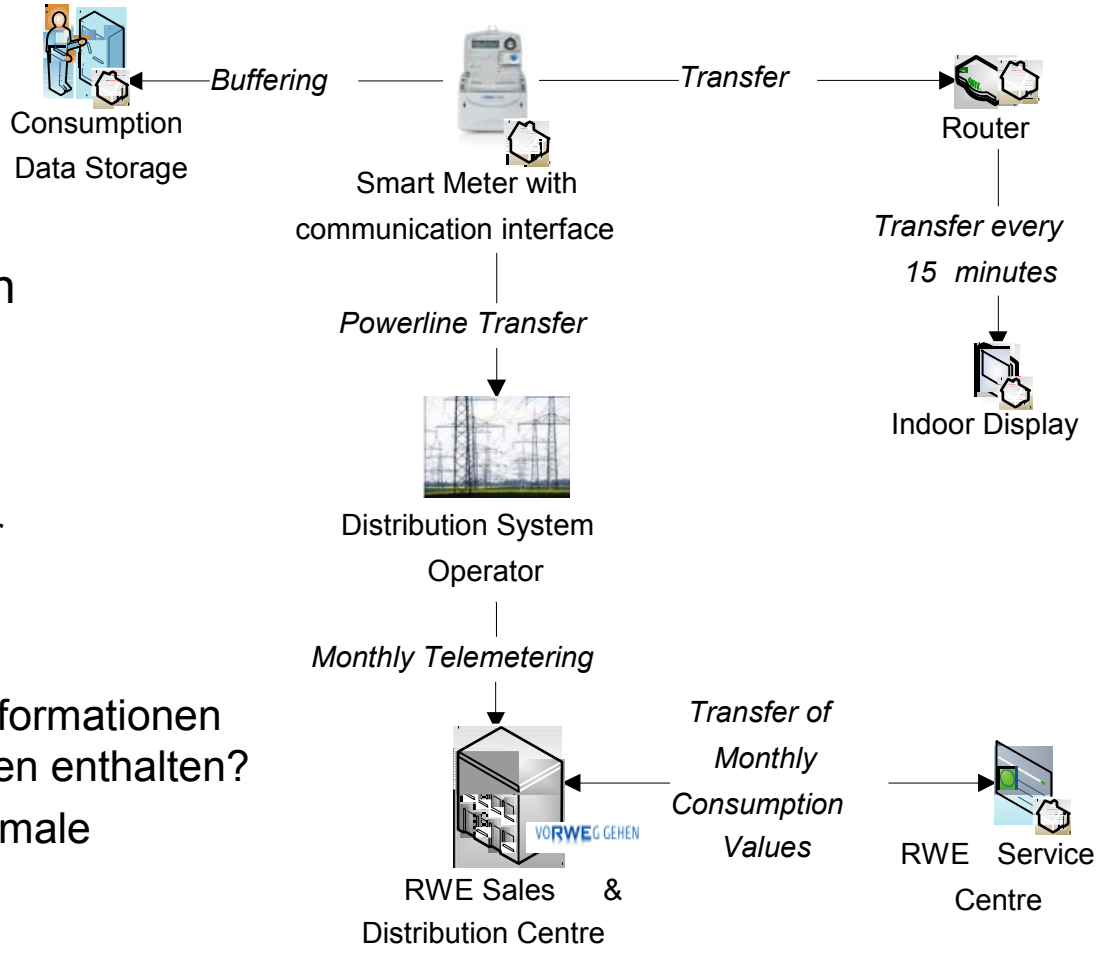
Verbund über alle Sensorknoten, die ähnliche Temperatur messen



- Problem: Wenn Anfrageergebnis offensichtlich falsch, welcher Knoten wars?
  - Knoten defekt
  - Übertragungsfehler
  - Hackerangriffe

Aktuelle Forschungsschwerpunkte (3/3)

- Datenschutz im Smart Grid
  - untereinander vernetzte Komponenten verarbeiten persönliche Daten
    - intelligente Stromzähler
    - Elektromobilität
    - intelligente Verbraucher
  - Forschungsfragen
    - Welche persönlichen Informationen sind in den Datenströmen enthalten?
    - Wie können diese Merkmale entfernt werden?



Beispiel: RWE

Lernziele der Vorlesung

- Ziele und Grundbegriffe der Informationellen Selbstbestimmung
- Erkennen, welche Vorgänge Datenschutz-relevant sind
- Bestimmung der Herausforderungen des Datenschutzes und ihrer Auswirkungen auf Gesellschaft und Individuen
- Anwendung aktueller Technologien zum Datenschutz, z.B. Methoden des Spatial & Temporal Cloaking
- Risikoabschätzung unbekannter Technologien
- Entwicklung und Bewertung geeigneter Maßnahmen zum Umgang mit diesen Risiken
- Reflektion des eigenen Umgangs mit persönlichen Informationen in vernetzten Informationssystemen

Gliederung der Vorlesung

- Motivation
- Gesellschaftliche Grundlagen
  - Exkurs: Datenschutzrecht
  - Öffentlicher Diskurs Vorratsdatenspeicherung
- Technische Grundlagen
  - Quasi-Identifier und Maße für die Anonymisierung
  - Perturbationstechniken und Kryptographie
- Angewandter Datenschutz
  - Datenschutzlösungen für Internet und Ubiquitous Computing
  - Ansätze wie Hippokratische Datenbanken
- Datenschutz-Praktikum im Labor

Karlsruher Institut für Technologie

Die Ausgangslage

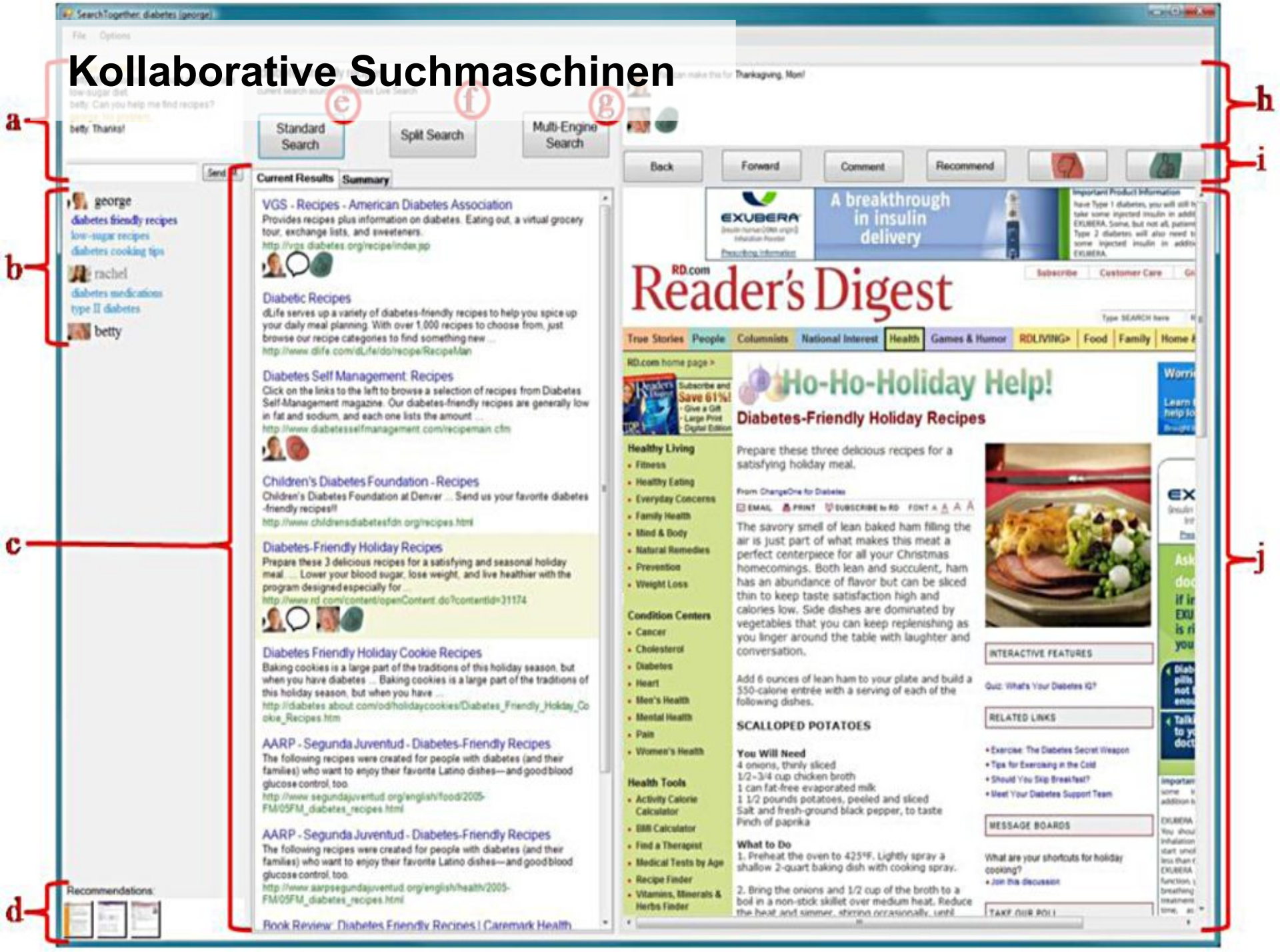
IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

Worum geht es in dieser Vorlesung?

- Sammeln, verarbeiten, speichern, abrufen und weitergeben von personenbezogenen Informationen in aktuellen und zukünftigen Informationssystemen

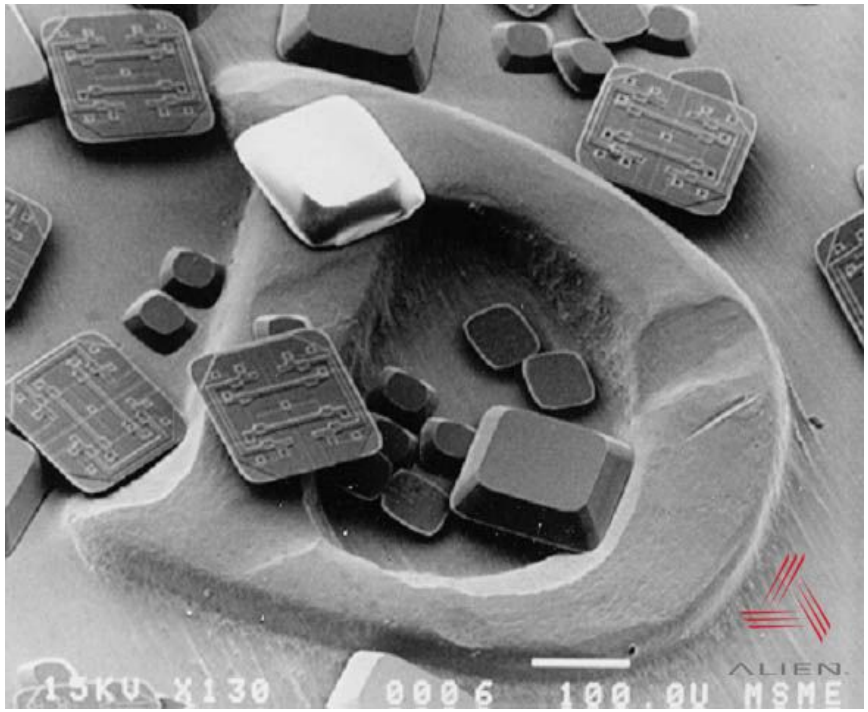
- Beispiele für relevante Technologien
  - Internet, Kollaborative Suche, Social Network-Portale
  - Sensornetze, RFID
  - Ubiquitous Computing, Location-Based Services
- Beispiele für relevante Anwendungen
  - Überwachung, Kontrolle
  - Data Mining, Collaborative Filtering
  - Intelligente Dienste im Alltag
  - Soziale Dienste, Web 2.0

Kollaborative Suchmaschinen



Sensornetze

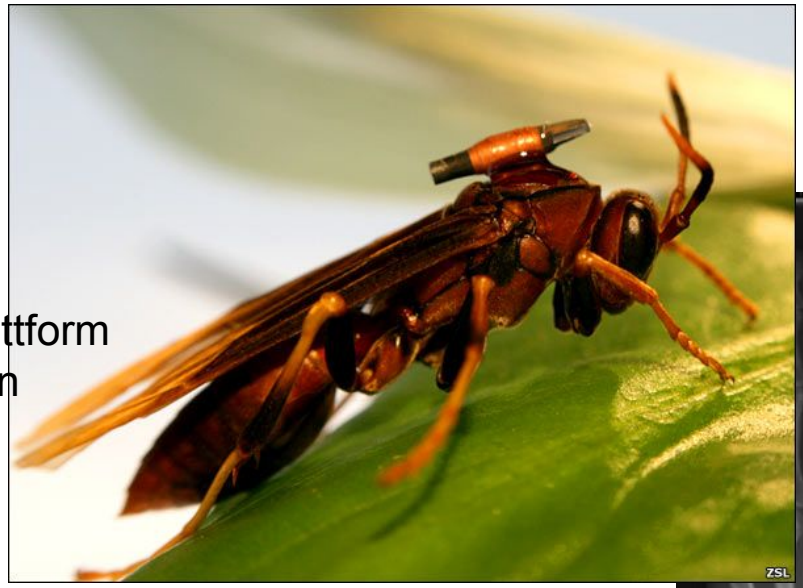
- “Intelligenter Staub” bis hin zu “Body Area Networks”
- Besonders problematische Anwendungsgebiete:
  - Grenzüberwachung
  - Verkehrsüberwachung
  - Gebäudemanagement
  - medizinische Kontrolle
- Hauptschwierigkeit heute: miniaturisierte Stromversorgung; Batterien geben die Größe vor



RFID chips on a 10 cent coin

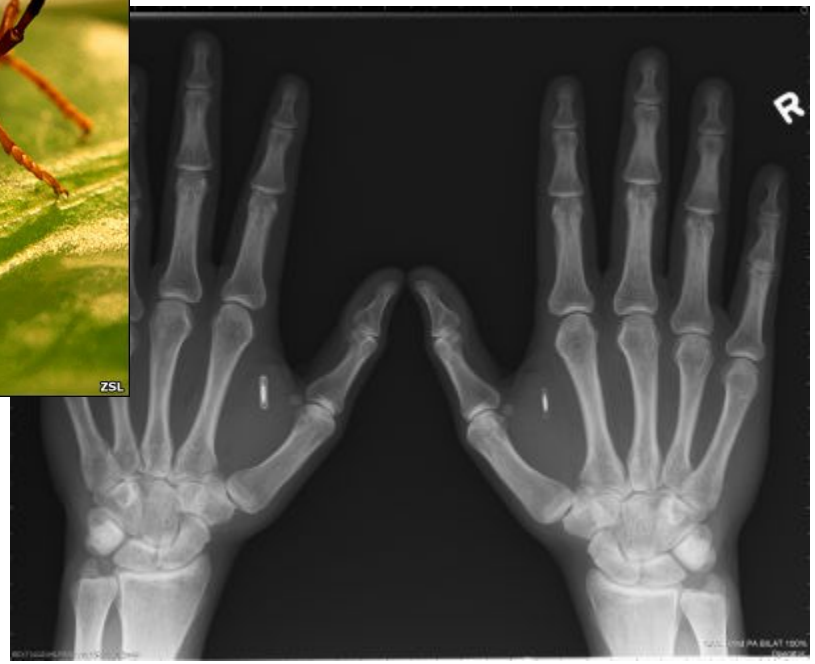
Technische Entwicklung, Beispiel RFID

2004:
Entwicklungsplattform für Sensorknoten
Siemens



2007: Wespe mit RFID-Tag, *Zoological Society of London*

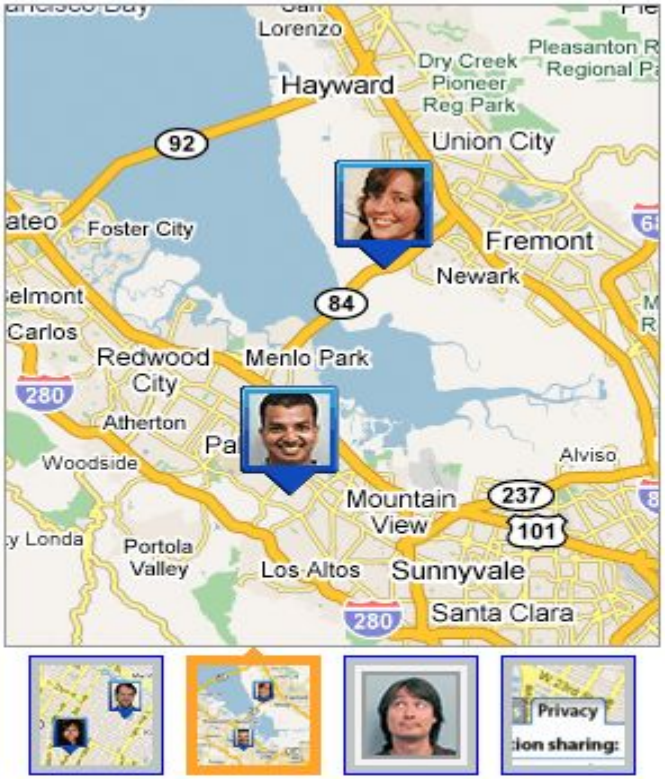
2011: in die Hand implantiertes RFID-Tag



Lokationsbasierte Dienste

Google Latitude

Introducing Google Latitude



My wife is on her way back from work. I'd better start preparing dinner now.

Learn more about Google Latitude

Watch a video

Discover other Google mobile products

See where your friends are right now

Enjoy Google Latitude on your phone, computer, or both.

Start using it on your phone

See your friends' locations and status messages and share yours with them.

Enter your number or visit google.com/latitude on your mobile web browser.

Send a link to my phone

United States

Will it work with my phone?

View it on your computer

See your friends' locations and status messages on a full screen even without a compatible phone or data plan.

Add Latitude to iGoogle »

Google

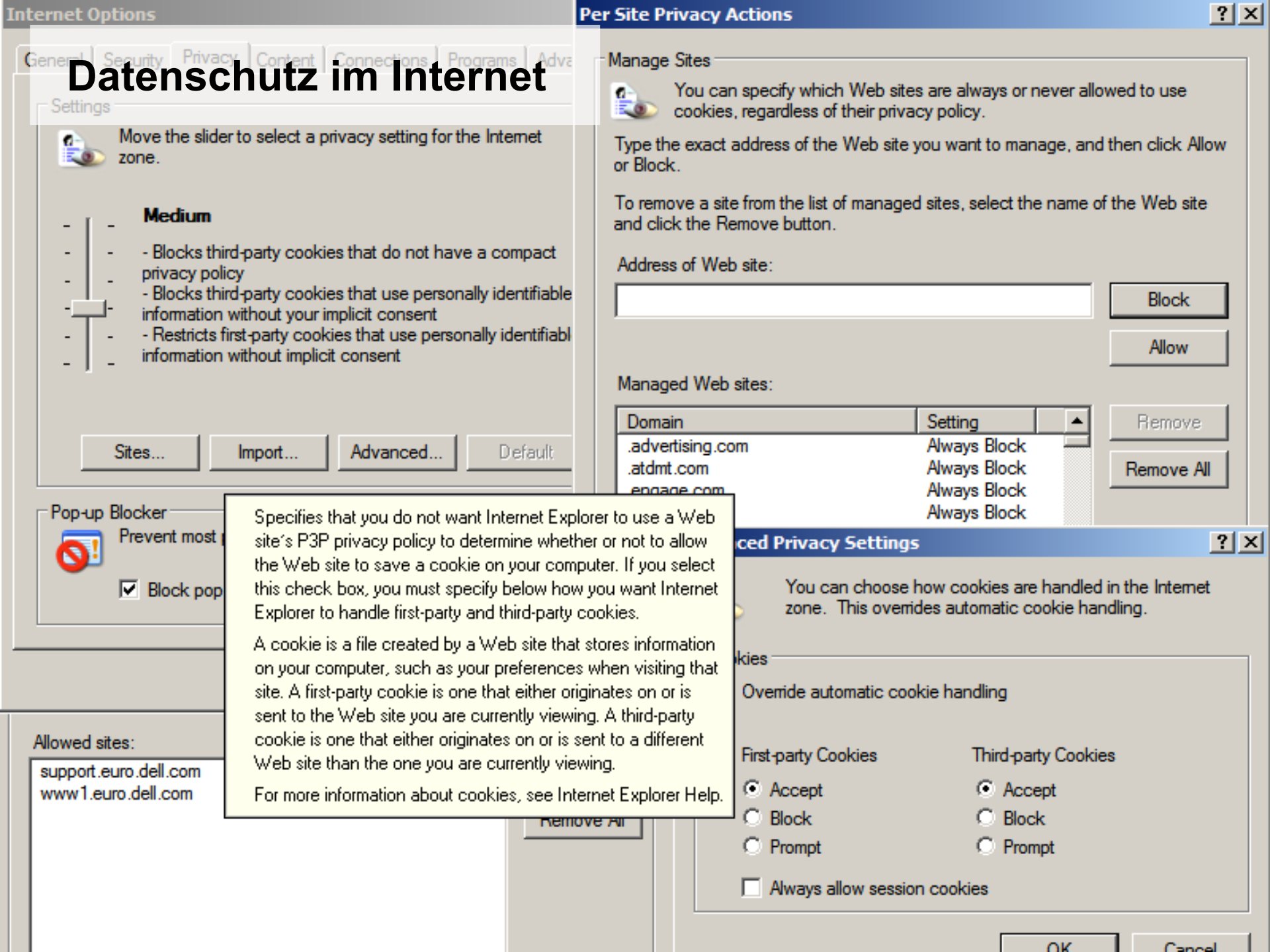
This service is free from Google; carrier charges may apply. The number entered on this page will only be used to send you a text message. It will not be linked to any Google services unless you've given us permission elsewhere.

RFID

- Jedes Objekt bekommt einen RFID-Chip aufgeklebt, der
  - über einige Entfernung berührungslos und ohne direkte Sichtlinie auslesbar ist, und
  - eine weltweit eindeutige ID speichert.

- Kurz vor der Einführung in den Massenmarkt
  - Hauptschwierigkeit: Preis der RFID-Chips

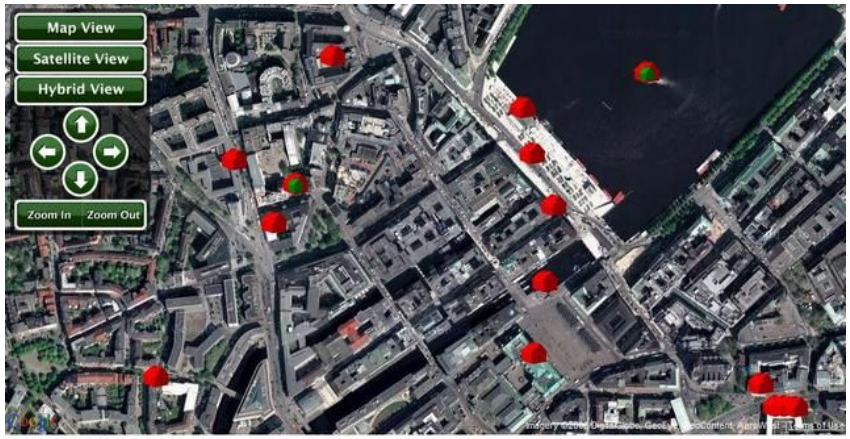
Datenschutz im Internet



Mashups

- Personenbezogene Daten aus unterschiedlichen Quellen

Girls Around Me:
Foursquare + Facebook +
Google Maps *(Bild: Zeit.de)*



Nearest Neighbors

Title	Distance	Votes	Rotten or Rad	Location
dicke titten!	0.12 Miles	0		N/A
hier kann man gar nicht richtig baden	0.12 Miles	0		N/A
GFK	0.13 Miles	0		N/A
kein	0.14 Miles	10		N/A
hier gaggt die ente gern	0.14 Miles	0		N/A

Rottenneighbor.com:
Google Maps + Soziales
Netzwerk *(Bild: Gulli.com)*

Und um was geht es nicht?

- Datenschutzprobleme aus dem letzten Jahrtausend
  - Behörden, Meldewesen, Finanzamt
- Interne Datenschutzprobleme von Unternehmen
  - Lidl-Skandal, Bahn-Skandal, Telekom-Skandal
- Datenschutz und Gefahrenabwehr
  - Terrorismus, Flugdatenübermittlung, Bundestrojaner

Karlsruher Institut für Technologie

Datenschutz: Wo liegt das Problem?

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

Schon die potentielle Kontrollierbarkeit...

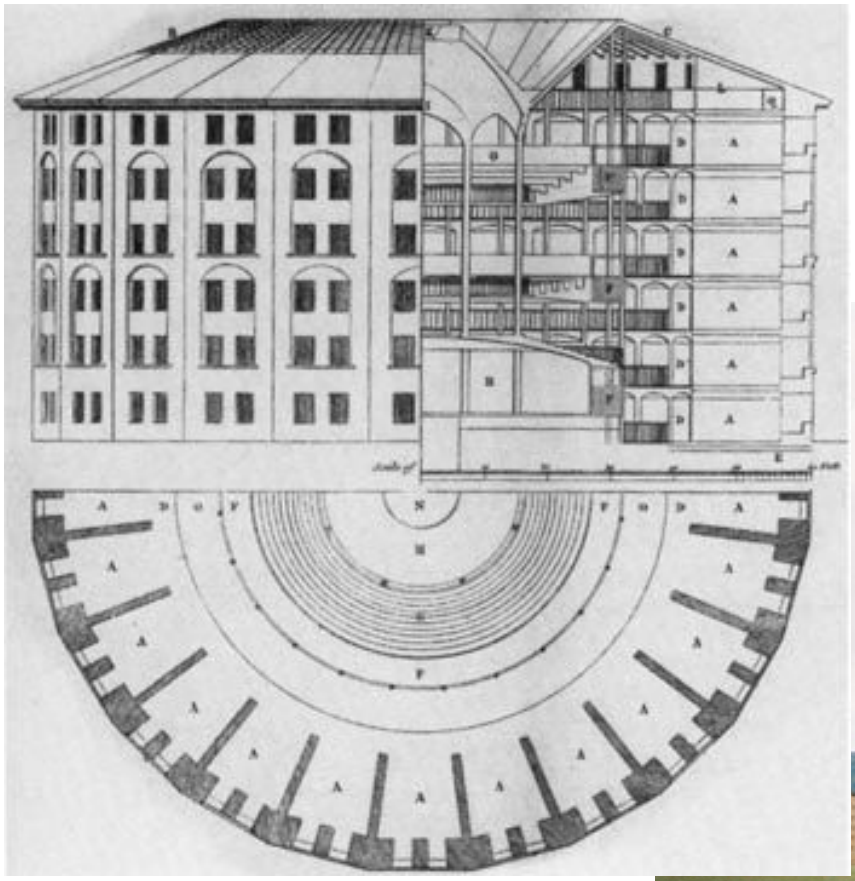
- ...reicht aus, um Menschen zu steuern.
  Es muss nicht mal eine Beobachtung stattfinden.

  → “Ich habe doch nichts zu verbergen!” ist Unsinn!

- Panopticon (1791)
  - Gefängnis-Modell nach den Entwürfen von Bentham;
  - ein einzelner Wärter kann in alle Zellen sehen,
  - die Gefangen wissen nicht, wann und ob sie beobachtet werden

    → Entspricht genau der Videoüberwachung

Panopticon, Aufbau und Umsetzung



Prison Presidio Modelo, December 2005

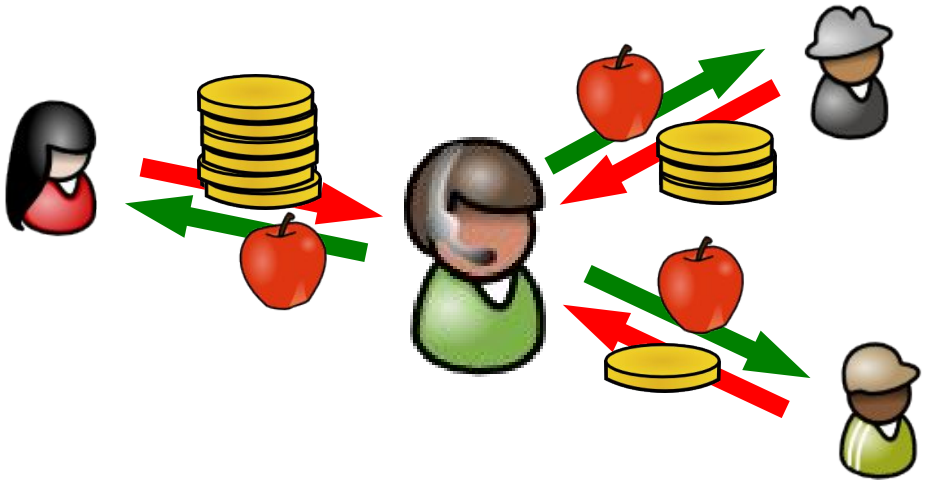
Bilder: Wikimedia Commons

Panopticon, Innenansicht

First-Degree Price Discrimination

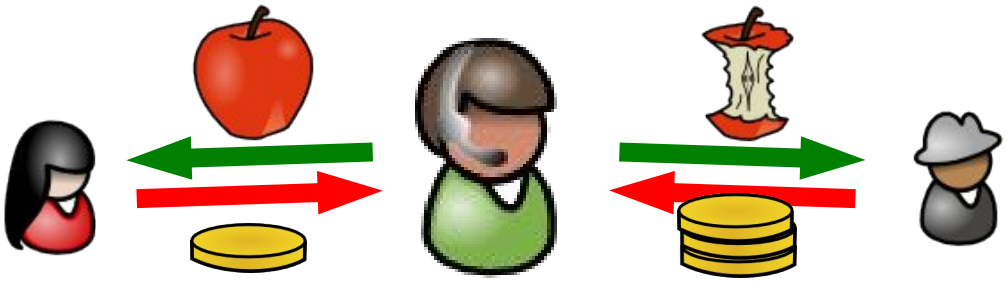
- auch “Perfect Price Discrimination”
- Händler kann
  - jeden Kunden individuell identifizieren,
  - jedem Kunden ein möglichst genaues Profil zuweisen,
  - und individuell den höchsten Preis bestimmen, den der Kunde für das Produkt zu zahlen bereit ist

→ Verlust an Privatheit wird direkt in Profit umgesetzt

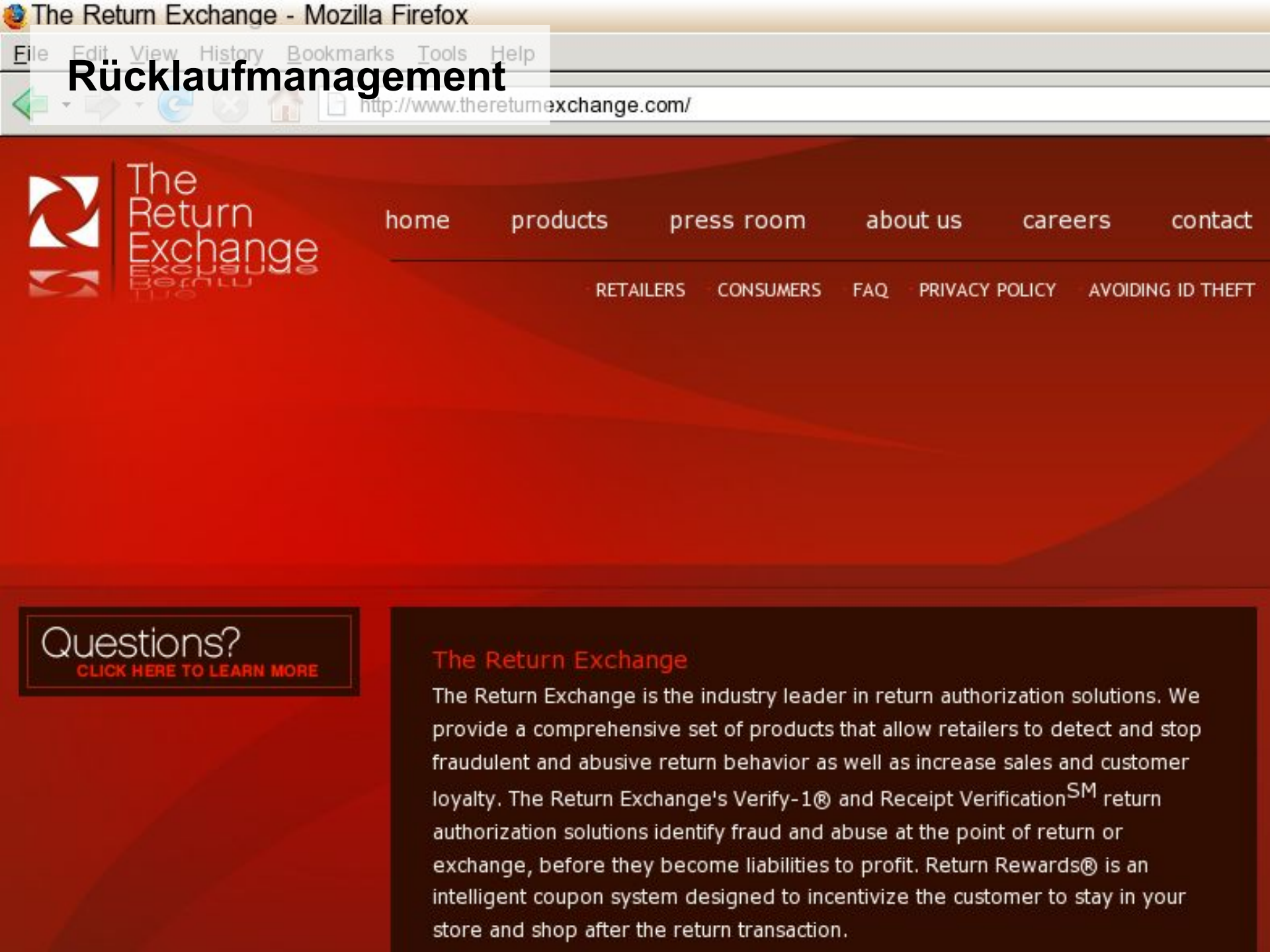


Den Kunden feuern

- Unerwünschte Kunden anhand statistischer Merkmale oder individueller Eigenschaften identifizieren
  - Rücklaufquote, Wohngegend, Zahl der Beschwerden
- Abschreckung, z.B.
  - unattraktive Preise
  - schlechten Service
- Je genauer der Kunde bekannt ist, desto sicherere Unterscheidung in guter/schlechter Kunde



Rücklaufmanagement



Was bedeutet Datenschutz?

- Datenschutz
  - Schutz personenbezogener Daten vor Mißbrauch
  - Informationelle Selbstbestimmung

- Wichtig für
  - die freie Entfaltung der Persönlichkeit
  - Handlungs- und Redefreiheit

- Nicht zu verwechseln mit Datensicherheit!
  - Vertraulichkeit, nur authentifizierte Nutzer
  - Verfügbarkeit, Zugriffe gewährleisten
  - Integrität, keine unbemerkten Änderungen

Personenbezogene Daten (1/4)

- Bundesdatenschutzgesetz, §3, Abs. (1)

Personenbezogene Daten sind **Einzelangaben** über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

  - Detailinformationen, also keine kumulierten Werte
    - Einzelangabe: Gehalt
    - Keine Einzelangabe: Durchschnittsgehalt der Bevölkerung

Personenbezogene Daten (2/4)

- Bundesdatenschutzgesetz, §3, Abs. (1)

Personenbezogene Daten sind Einzelangaben über **persönliche oder sachliche Verhältnisse** einer bestimmten oder bestimmbaren natürlichen Person

  - persönliche Verhältnisse:
    - Lebensumstände, Hobbies, politische Einstellung, medizinische Daten, Familienstand etc.
  - sachliche Verhältnisse:
    - Besitz, Einkommen, Grundeigentum etc.

Personenbezogene Daten (3/4)

- Bundesdatenschutzgesetz, §3, Abs. (1)

> Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer **bestimmten** oder bestimmbaren **natürlichen Person**

  - bestimmte Person
    - eindeutig identifizierbar, z.B. über den Namen oder die Personalausweisnummer
  - natürliche Person
    - juristische Personen (Körperschaften, Unternehmen, Gesellschaften) haben keine Persönlichkeitsrechte
  - Anmerkung: Es geht um die Person selbst, also nicht nur um den Namen. Der Name ist nur eine mehrerer Möglichkeiten, eine Person zu identifizieren.

Personenbezogene Daten (4/4)

- Bundesdatenschutzgesetz, §3, Abs. (1)

> Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder **bestimmbaren** natürlichen **Person**

  - bestimmbare Person (unscharfer Rechtsbegriff)
    - Von wem kann ein Datensatz mit wieviel Aufwand einer Person zugeordnet werden?
    - Beispiel:
      - feste IP-Adresse: kann Person eindeutig bestimmen
      - dynamische IP-Adresse: strittig, Internetprovider kann Person bestimmen, Webseitenbetreiber normalerweise nicht

Informationelle Selbstbestimmung

- Ziel: Die individuelle Selbstdarstellung gegenüber anderen selbst definieren
  - Ausprägung des allgemeinen Persönlichkeitsrechts, abgeleitet vom Grundgesetz
  - selbst festlegen, wer über welche persönlichen Informationen verfügt
    - keine Unterscheidung zwischen mehr oder weniger sensiblen Informationen → **es gibt keine belanglosen persönlichen Daten!**
  - Selbstbestimmung mit Einschränkungen
    - bei überwiegendem Allgemeininteresse,
      Kriminalität, Terrorismus, Steuererklärung, Fahrzeugregister,
      Einwohnermeldeamt,
      Wählerregister etc.

Der Begriff “Privatsphäre”

- *“Privatsphäre” ist ein Anachronismus*
  - privater Lebensraum, Privatleben, vertrauliche Informationen, häusliche Geborgenheit vs.
    öffentlicher Raum mit Gemeinschaftsinteressen
  - strenge Abgrenzung: Privatsphäre ist zu schützen, öffentliche Sphäre steht der Gesellschaft offen
  - Ziel des Modells: “Einmischung in die privaten Lebensbereiche” verhindern, Privates bleibt privat

- Heute: Sphärenmodell ist überholt
  - es geht um den **Personenbezug** als wesentliches Kriterium der Schutzwürdigkeit von Daten
    - erheblich weiterreichende Schutzziele!
  - Daten der “öffentlichen Sphäre” sind schutzwürdig, sofern nicht vom Betroffenen absichtlich veröffentlicht

Karlsruher Institut für Technologie

Historischer Abriß zum Datenschutz

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

Datenschutzprobleme folgen Technologie

- Mitte 19.Jh: Zeitungen und Zeitschriften
- 30er: Bürokratisierung im NS-Regime
- 60er: Anfänge der elektronischen Datenverarbeitung
- 90er: Siegeszug von PC und Internet

Im Fokus der Vorlesung:

- Heute
  - Verarbeitung personenbezogener Daten ohne Zweckbindung, Online-Communities und Soziale Netzwerk-Portale
- Zukunft
  - Datenverarbeitung wird (noch) unsichtbar(er)
    Ubiquitous Computing, Pervasive Computing, RFID
  - Unklare Verantwortlichkeiten durch starke Entkopplung von Datenerhebung, -verarbeitung, -nutzung
    - Cloud Computing, „Social Information Processing“

Mitte 19. Jh: Zeitungen und Zeitschriften

- Boulevardpresse in Nordamerika blüht auf, mit geringer Verzögerung auch in Europa
  - Millionenauflagen erhöhen die Reichweite von Informationen, auch Klatsch und Tratsch
- Datenschutz: kontrollieren, was in die Zeitung darf
  - Privatsphäre
    - Heim und Herd, Informationen aus dieser Sphäre privat
  - öffentliche Sphäre
    - auf der Straße und in der Öffentlichkeit, keine Privatheit
- 1890: Warren and Brandeis, The Right to Privacy, Harvard Law Review
  - Privacy als “das Recht, in Ruhe gelassen zu werden”

30er: Bürokratisierung im NS-Regime

- Ausweitung der Bürokratie im NS-Regime
  - papierne Aktenberge enthalten detaillierte Informationen zu jedem Bürger
- Bürokratisierung von Unterdrückung und Völkermord
  - Judenverfolgung durch Eintrag der Religionszugehörigkeit in den Melderegistern
- Datenschutz gilt nicht für Regierung

Deutschland nach dem 2. Weltkrieg

- Ziel: Bundesrepublik Deutschland soll das Gegenteil vom NS-Reich werden
- Ansatz: *Förderalismus*
  - Aufsplitterung von staatlicher Gewalt incl. staatlichem Wissen
  - klare Aufgabenteilung, klare Beschränkungen
- Viele hoheitliche Aufgaben sind Ländersache
  - Polizei, Verwaltung, Rechtsprechung, etc.
  - keine Verknüpfung unter den Datenbeständen (Karteikarten; daher auch kaum praktikabel)
- Problem: Ineffizientes und teures System, “Reibungsverluste” bei Verwaltung kleiner Einheiten

60er: Anfänge der el. Datenverarbeitung

- Computer sind teuer
  - wenig elektronische Datenverarbeitung, Mainframes, kaum vernetzte Datenbanken
  - Nur Staat und sehr wenige Großunternehmen können sich Datensammlungen in großem Stil leisten
- ein Großteil der Datenverarbeitung erfolgt immernoch mit Karteikarten und Papierakten
- Mangelnde Datenverarbeitungskapazität ist eine natürliche Grenze für die Speicherung, Verknüpfung und Auswertung personenbezogener Daten
- Datenschutz als Schutz des Bürgers vor dem Staat
  - Lehre aus der NS-Zeit

1974: Privacy Act

- Reaktion auf den Datenmißbrauch der Nixon-Ära
- “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains..”, *Public Law No. 93-579, 88 Stat. 1897 (1974), USA*
  - Verbot mit Erlaubnisvorbehalt
    - schriftliche Zustimmung erforderlich
  - definiert eine Reihe von Ausnahmen
    - statistische Zwecke, Verwaltungsaufgaben, Nachforschungen von Regierungsorganisationen

Deutschland der 70er Jahre

- 1970: Hessen verabschiedet als erstes Bundesland ein Landesdatenschutzgesetz
  - Zugriffsschutz elektronisch verarbeitbarer Daten
  - Verschwiegenheit der datenverarbeitenden Stellen
  - Einrichtung eines Landesdatenschutzbeauftragten
- 1977: erstes Bundesdatenschutzgesetz
  - Erforderlichkeitsgrundsatz bei der Datenerhebung
  - Personenbezogene Daten nur erheben und verarbeiten, wenn Gesetz oder freiwillige Zustimmung
  - kaum Einschränkungen privater Datenverarbeitung

Die geplante Volkszählung 1982/1983

- Ziel: Verminderung des Verwaltungskostenanteils, Rationalisierung
- Ansatz:
  - Volkszählung, erhobene Angaben bleiben geheim
  - Abgleich von Name und Adresse mit polizeilichen Melderegistern
  - Weitergabe von Angaben ohne Nennung von Name und Adresse an Ministerien und Gemeinden
- Kritik: geheime Angaben sollten miteinander verknüpft und ohne Kenntnis der Betroffenen an unbekannte Staatsorgane weitergegeben werden
  → *Massenproteste*

Das Volkszählungsurteil 1983

- Das Bundesverfassungsgericht hat geurteilt
  - *“Jeder kann selbst über die Weitergabe und Verwendung persönlicher Daten entscheiden, er kann bestimmen, in welchen Grenzen Lebensumstände zu offenbaren sind."*
  - Abgeleitet aus Artikel 1 und 2 Grundgesetz:
    - „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen, ist Verpflichtung aller staatlicher Gewalt.“
    - „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“
- Erstmalige Einführung des Begriffs *“Informationelle Selbstbestimmung”*

90er: Siegeszug von PC und Internet

- PCs und Server stehen in Verwaltung und Unternehmen
  - Rechenleistung und Speicherkapazität sind billig
  - Internet hat sich durchgesetzt
- Unternehmen sind im Besitz großer elektronischer Datenbanken
  - automatische Datenverarbeitung im großem Umfang
  - Data Warehousing und -Mining auf Kundendaten wird Standardwerkzeug
  - elektronisches Scoring und Ranking von Kunden
- Globale Großunternehmen bilden sich
  - Globale Datenübertragung
- Datenschutz als Schutz vor Unternehmen

1990: Neufassung Bundesdatenschutzgesetz

- Resultiert aus den umfangreichen Diskussionen im Anschluss an Volkszählungsurteil
  - Transparenz in der Datenverarbeitung
  - Anspruch auf Auskunft, Berichtigung, Löschung
  - explizite Berücksichtigung von staatlichen, privaten Unternehmen sowie Privatunternehmen mit staatlichem Auftrag
  - Grundrecht auf Informationelle Selbstbestimmung

1995: Europäische Datenschutzrichtlinie

- Richtlinie 95/46/EG muss von allen EU-Mitgliedsstaaten in nationales Recht überführt werden
  - 2001 Umsetzung in Deutschland ins BDSG
- Harmonisierung des Datenschutzrechts in der EU
  - Hohe Datenschutzstandards in allen EU-Ländern
  - für neue DS-Gesetze werden Risikianalyse, Vorabkontrolle, Technikfolgenabschätzung vorgeschrieben
  - erleichtert grenzüberschreitenden Datenverkehr in der EU, Datenübermittlung an Nicht-EU-Länder nur, wenn dort angemessenes Datenschutzniveau
    → USA: Safe Harbor Programm
- Datenschutz wird Grundrecht

Novellierung des BDSG 2009

- Novelle 1: transparentere Auskunfteien, Scoring- und Kreditinstitute
  - Stärkung der Verbraucherrechte im Bezug auf finanzielle Belange (Kreditwürdigkeit), insbes. hinsichtlich automatisierter Scoring-Verfahren
- Novelle 2: Adresshandel, Markt- Meinungsforschung
  - Verbesserungen am BDSG aufgrund zahlreicher Skandale in der Privatwirtschaft
- Novelle 3: Auskunftspflichten für Daten zur Kreditwürdigkeit
  - Auskunfteien müssen Anfragen aus dem europäischen Ausland beantworten; Umsetzung der Zahlungsdiensterichtlinie (2007/64/EG)

Szenario: Heute

- Alltag breiter Bevölkerungsschichten von elektronischen Medien durchdrungen
  - Internet, Mobiltelefone, PDAs
- Allgegenwärtige und bezahlbare Vernetzung
  - 2011: >=1 MBit/s für 98,7% aller deutschen Haushalte
  - UMTS flächendeckend in allen größeren Städten
- Web2.0 führt zu einem Anstieg bei der Preisgabe personenbezogener Informationen durch Betroffenen

- Relevante Technologien
  - Internet und Cloud Computing
  - „Soziale“ Dienste: kollaborative Suchmaschinen, Social-Network-Portale
  - Ubiquitous Computing: Lokationsbasierte Dienste, Smartphones

Szenario: Morgen

- Datenverarbeitung tritt immer mehr in den Hintergrund
  - Ubiquitous Computing wird durch Smart Grid massentauglich
    - Intelligente Alltagsgegenstände
    - automatische Unterstützung alltäglicher Verrichtungen
    - Dienste versuchen Nutzerwünsche zu “erraten”
- Verantwortlichkeiten werden (noch) unklarer
  - Cloud Computing-Dienste verarbeiten und speichern persönliche Daten
  - Viele Anwendungen werden „sozial“

- Relevante Technologien
  - Smart Grid: Intelligente Stromzähler, intelligente Geräte, Elektrofahrzeuge, zahlreiche Dienstleister mit Zugriff auf persönliche Daten
  - allumfassende Vernetzung: Stromverbraucher, Computer, Smartphones, Sensornetze

Karlsruher Institut für Technologie

Zusammenfassung

IPD, Systeme der Informationsverwaltung, Nachwuchsgruppe „Privacy Awareness in Information Systems“

Prinzipien des Datenschutzes

- Jeder Bürger soll selbst bestimmen, und
- Jeder Bürger soll wissen,
  - wer was wann und unter welchen Bedingungen
    - über ihn weiß.
    - über ihn in Erfahrung bringen darf.

- Ausnahmen nur auf gesetzlicher Basis
  - wenn das Interesse Dritter bzw. der Allgemeinheit schwerer wiegt als die Schutzinteressen des Betroffenen

Klassische Datenschutz-Schwerpunkte

- Schutz des Bürgers vor dem Staat
  - Recht auf freie Meinungsäußerung wird bedeutungslos, wenn Regierung den Sprecher im nachhinein identifizieren (und abstrafen) kann
    → **Datenschutz wichtig für Demokratie**

- Schutz des Bürgers vor privaten Unternehmen
  - Sind die individuellen Vorlieben und Absichten des Käufers bekannt, wird perfekte Preisdifferenzierung und Manipulation des Käufers möglich
    → **Datenschutz ist Kundenschutz**

Neue Schwerpunkte der letzten Jahre

- Schutz des Bürgers vor dem Dienstanbieter
  - Verknüpfung und Mining von personenbezogenen Daten, die als “Nebenwirkung” moderner Dienste anfallen
    (Beispiel: persönliche Daten über Suchvorgänge preisgeben)
  - Daten werden ohne nachzudenken an unbekannten Orten gespeichert
    (Beispiel: transparente Infrastruktur durch Cloud-Computing-Dienste)
    → **Verbleib persönlicher Daten nachvollziehen**
- Schutz des Bürgers vor dem Bürger
  - Werden in Online-Communities private Details zu Dritten preisgegeben, lassen sich Persönlichkeitsprofile von Unbeteiligten erstellen.
    → **Kontrolle über persönliche Daten behalten**

Literatur

[1] BDSG, http://bundesrecht.juris.de/bdsg_1990/index.html

Ich hab' nichts zu verbergen!

Blutgruppe B, Herzinfarktrisiko 14%, KV-Datensatz
(Genanalyse) liegt vor, Krankenversicherung: Standard,
Zusatzversicherung angeboten (File 23A18)
Risikoklasse 4 - (Nachuntersuchung erforderlich
in Q8, Verdacht auf KV-Risiko Stufe 3)
Drogenkonsum: Nicht aktuell.
Alkoholkonsum mittel bis niedrig,
Einkommen €1434;-, RV, PV, KS, VWL
Kredit: DB, €40.000, Konto: €-729
Zahlungsmoral: nachlässig, Versand auf Rechnung
einstellen, Kundennr: 393848, Punkte: 2930,
Umsatzpotential nicht ausgeschöpft.
Interessensprofil Musik/Buch: liegt vor
Interessensprofil Reisen: liegt vor,
Bürgerklasse 3 (Normal, Wiedervorlage, geplant 2009,
ID-Code C89A839A) Soziales Umfeld: Thomas B.,
Kerstin A., Verena L. (siehe Datensatz B33421)
Arbeitgeber K8273-23, Datenbankabgleich: OK
Verspätungen: 4, Abmahnung: Nein, Auto: Ford Fiesta,
TÜV, Teilkasko, Verkehrsdelikte: 2 (leicht) 0 (schwer)
Risikostufe: 3, Tendenz fallend, Maut-ID A38-92384
Fahrzeugbewegungsdaten: liegen vor ab 04/2006
Politische Ausrichtung: SPD (bis 2005), Seit 2005
Nichtwähler, Teilnahme an AK-Demo 2005 (Video #0232-4)

...bis auf meine Privatsphäre.

www.datenschutzzentrum.de ULD