Privacy im Zeitalter von Ubiquitous Computing

Doktorandenseminar

Ubiquitäre Information

ETH Zürich, WS 2000/01
Langheinrich, Moschgath, Vogt

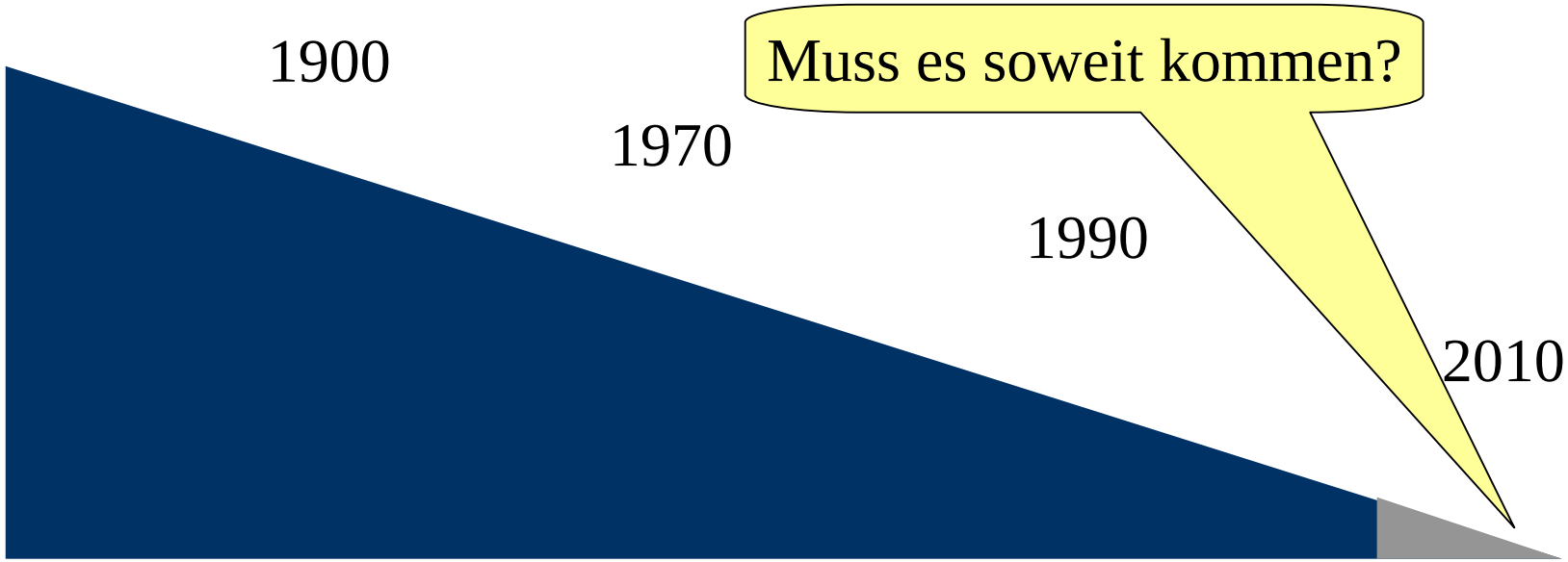
Was ist „Privacy“?

- Definition (Versuch):
  Kontrolle über (persönliche) Daten
- Merkmale:
  - Personenbezogenheit (direkt und indirekt)
  - Sensitivität (subjektiv)
  - Kontrolle (bspw. Verbreitung)
- Aufhebung der Personenbezogenheit ➔ Anonymisierung
- Verlust der Sensitivität ➔ Daten wertlos
- Kontrollverlust ➔ Privacy geht verloren - ***für immer***

Welche Daten sind privat?

- Beispiele: *Medizinische Daten, Kontonummer, Alter der Kinder, Telefonnummer, Adresse, Automarke, Name, Strafregister, Liebschaften, Charaktereigenschaften, Vorlieben, Leidenschaften, Geschmack, Freizeit,...*
- Begriff von „Privatheit“ ist individuell verschieden
- ... und situationsabhängig
- Unterschiedliche Auffassungen: USA/Europa

Verlust der Privatsphäre?



Persönlicher, physischer Kontakt, Briefform

Telefon

Zeitung, Fernsehen

EDV

Kreditkarten

Datenaustausch u. -abgleich

Globale Vernetzung, WWW

Kamera-Überwachung

Ubiquitous Computing & Networking

Kommunikations- u. Informationstechnik →

Bedeutung von Privacy

- Verlust der Privacy kann
  - ein Leben zerstören
  - Ruf schädigen
  - Verbrechen ermöglichen (identity theft)
  - Personen transparent und berechenbar machen
  - ...
- Gegenmassnahmen
  - Geschlossene Türen, Vorhänge
  - Soziales Verhalten (beruhend auf gegenseitigem Respekt)
  - Vertraulichkeit
  - Datenschutz, Anonymisierung

Bedeutung von Privacy (2)

- Preisgabe von persönlichen Daten ermöglicht aber auch:
  - Massgeschneiderte Angebote
  - Einkaufen von zuhause
  - Schutz vor Verbrechen
  - Leben retten
  - ...

Vereinfachte Informations-erhebung und -verarbeitung

- Beispiel: Kreditkarten
- Transaktionen...
  - werden gespeichert
  - spiegeln reales (Kauf-)Verhalten wider
  - werden ausgewertet, verkauft, (aus)genutzt
  - geben ein Bild der Person ab?

Die Gegenwart: Das Web

- Persönliches Verhalten spiegelt sich im Cyberspace:
  - Konsumverhalten (amazon.com)
  - Freizeit (my.yahoo.com)
  - Unterhaltung (zone.com)
  - Urlaub (expedia.com)
  - Arbeit (mywork.com)
  - Kommunikation (deja.com)

Ubiquitous Computing

- Der Mensch steht im Mittelpunkt
  - Personalisierte Dienste
  - Kontextabhängigkeit (do what I want)
  - Ergonomie
- Allgegenwärtiger Zugriff auf Informationen
  - Alles ist immer und überall online
- Neue Interaktionsformen
  - werden möglich
  - sind notwendig
- Mobilität
  - Aufenthalt in „fremden“ Umgebungen

Folgen des Ubicomp

- (Fast) alle Interaktionen in der realen Welt werden über (vernetzte) Computer ausgeführt
- Vision: 3D-Weltmodell
  - Abbild des Menschen im Cyberspace
    Umfassende Beobachtung (technisch) möglich
  - Beeinflussung der physischen Welt (in Echtzeit) am Computer
- Nichts wird vergessen

Werkzeuge - Übersicht

- Privacy:
  „Kontrolle über persönliche Daten“
- Werkzeuge zur Wahrung der Privacy:
  - Anonymisierung
  - Privacy Management
  - Juristische und gesellschaftliche Kontrolle

Anonymisierung

- Aufhebung der Personenzuordnung
  - „Weiche“ Anonymisierung
    z.B. anonymous ftp
  - „Harte“ Anonymisierung
    z.B. Mixe, anonymizer.com
- Beschränkte Anwendbarkeit
  - Anonymität nicht immer gewünscht

Privacy Management

- Ziele
  - Kontrolle (Wer? Wann?)
  - Transparenz (Warum? Verwendung?)
  - Protokollierung
  - Pseudonymisierung
- Ansätze
  - Infomediaries (www.privacybank.com)
  - P3P

Soziale Kontrolle

- Juristische und gesellschaftliche Kontrolle
  - Gesetzl. Vorschriften für Betreiber zum Schutz der Benutzer
  - Aufsichtsbehörden (DSB, FTC)
  - Marktmechanismen (z.B. Doubleclick-Fall)
  - Zertifizierungsprogramme

Selbstdatenschutz

Internet-Techniken

„Low-tech“ Lösungen

- Nur in Cyber-Cafés surfen
- ISP ohne Anmeldung (z.B.Sunrise freecall)
- Kostenloser e-mail account statt ISP
- E-mail Header, IP-Adresse fälschen
- ... Und natürlich niemals personenbezogene Daten ausgeben!

Beispiel Internet

Client-Anonymität

- Entspr. konfigurierter Proxy
- **Anonymizer.com**
- Rewebber.com
- ...

Server-Anonymität

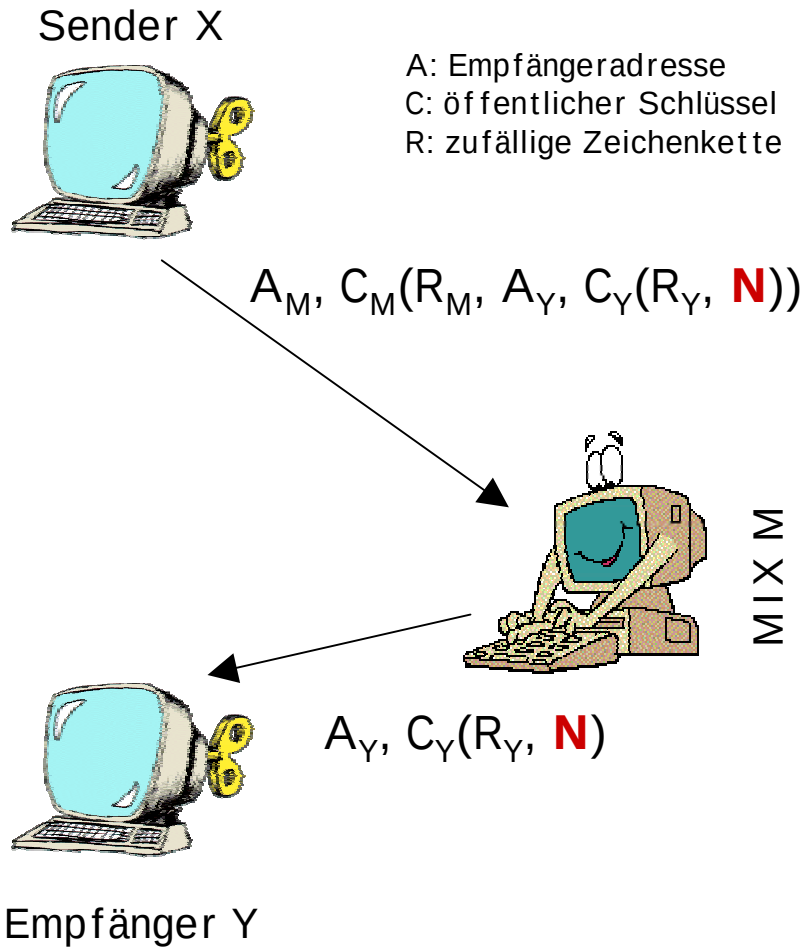
- **Rewebber.com**
- Rewebber Network und TAZ
- ...

Zusätzliche Anonymität der Kommunikation

- **Onion-Router**
- **Crowds**
- Freedom (Zero-Knowledge Inc.)
- Web-Mixe (TU Dresden)
- Web-Incognito (Privada)
- ...

MIX-Modell von Chaum

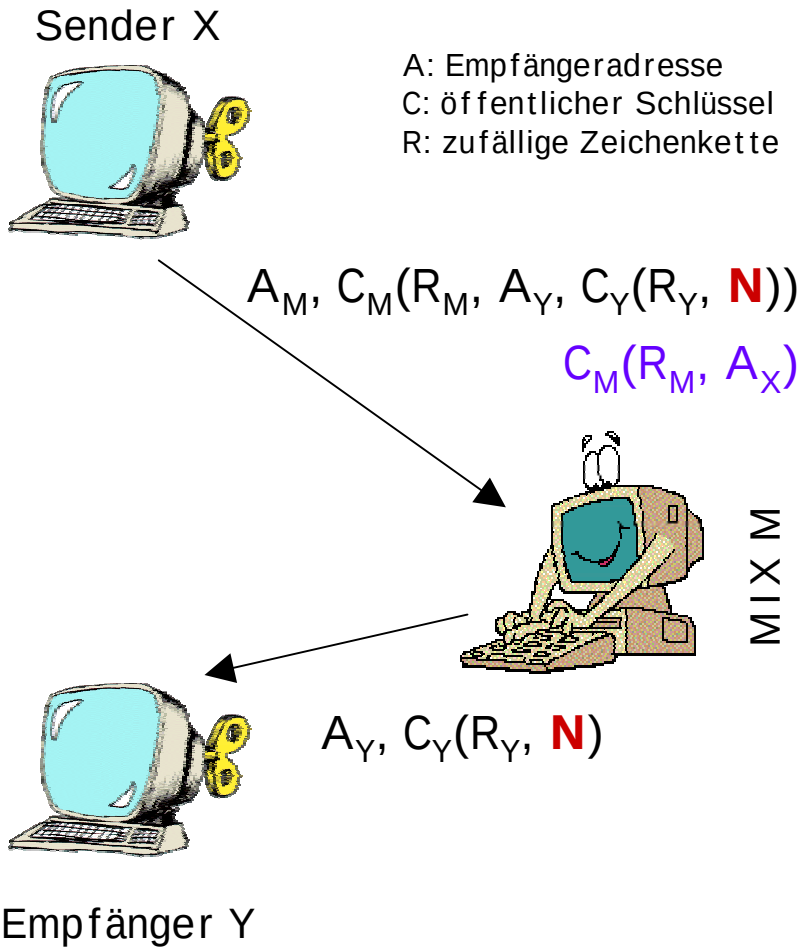
- von David Chaum (1981)
- Ein MIX hat die Aufgabe, eine Nachricht von Sender X an Sender Y weiterzuleiten und sich selbst als Absender auszugeben
- asymmetrische Verschlüsselung
- MIX-Kaskaden, MIX-Netze



MIX-Modell von Chaum

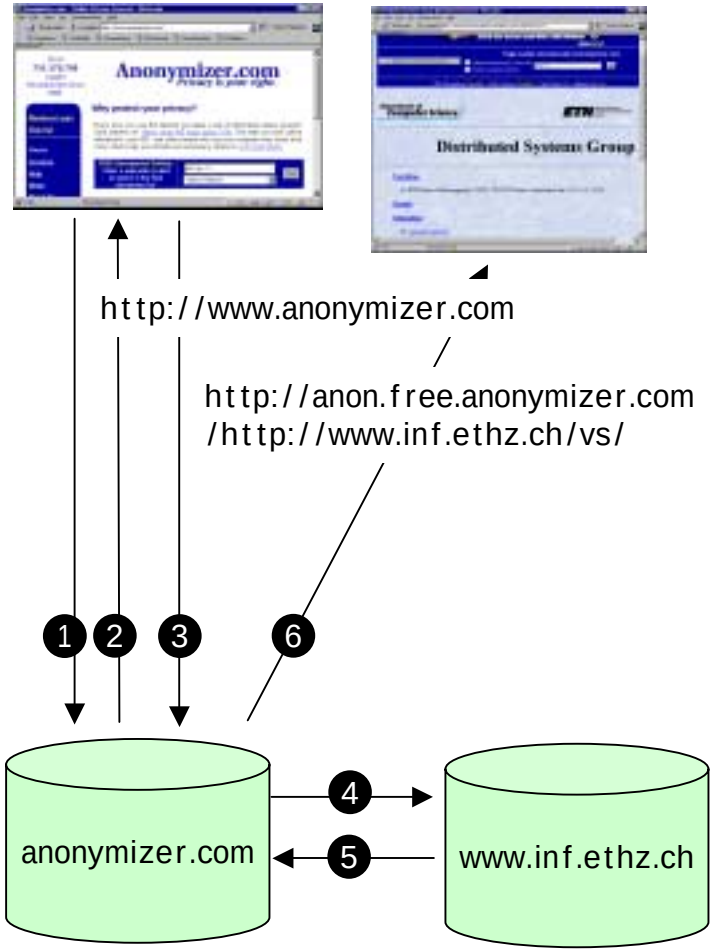
Erweiterung: Anonyme Rückadressen

- von David Chaum (1981)
- Ein MIX hat die Aufgabe, eine Nachricht von Sender X an Sender Y weiterzuleiten und sich selbst als Absender auszugeben
- asymmetrische Verschlüsselung
- MIX-Kaskaden, MIX-Netze



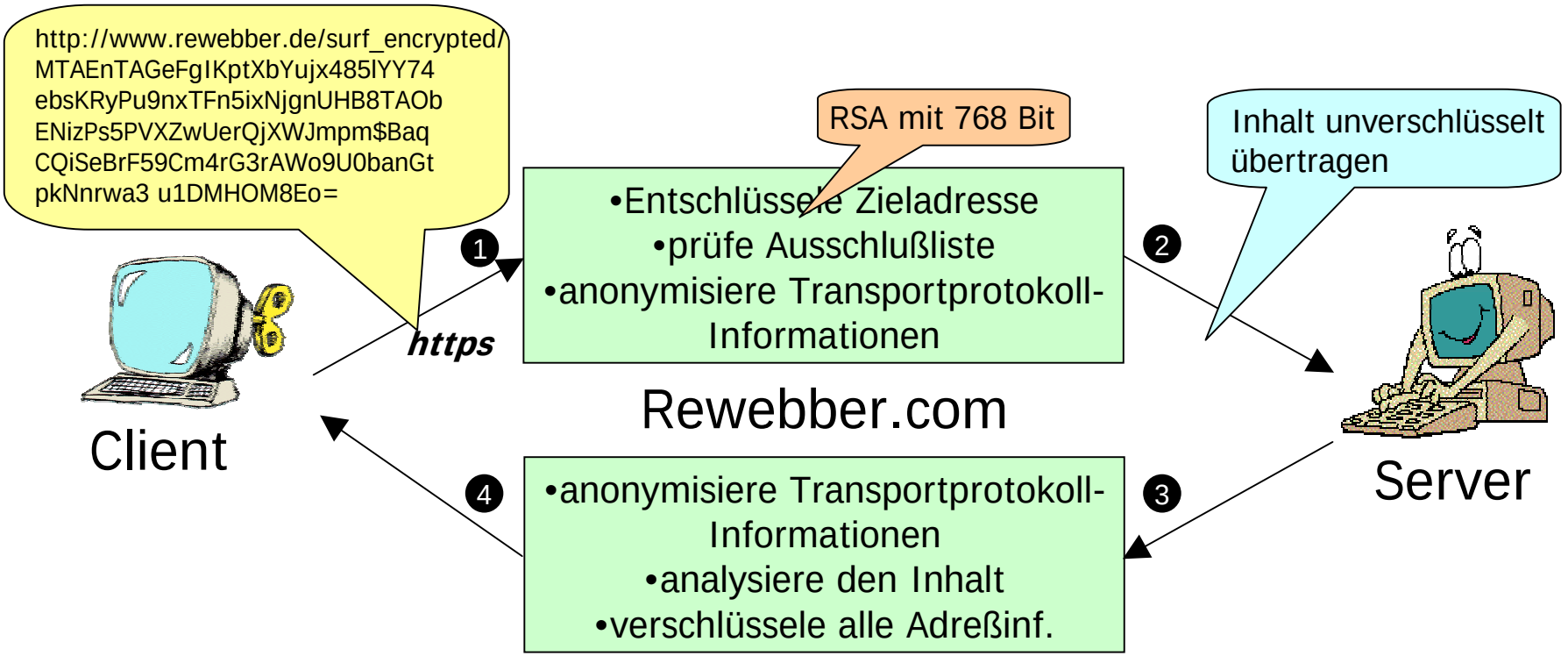
Proxies & Anonymizer.com

- **Proxies** werden in erster Linie zur Zwischenspeicherung von Dokumenten und damit zur Vermeidung von unnötigem Verkehr eingesetzt
- Der **Anonymizer.com** ist ein Proxy, der keine Zwischen-speicherung durchführt
- Kein Schutz gegen Verkettung

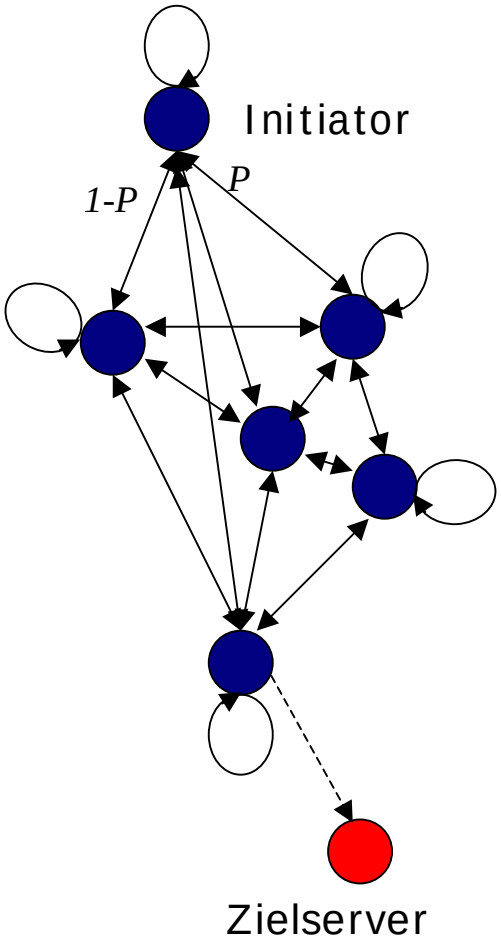


Rewebber.com

- Vormals „Janus“ (Fernuni Hagen)
- Client- und Server-Anonymität, Unbeobachtbarkeit

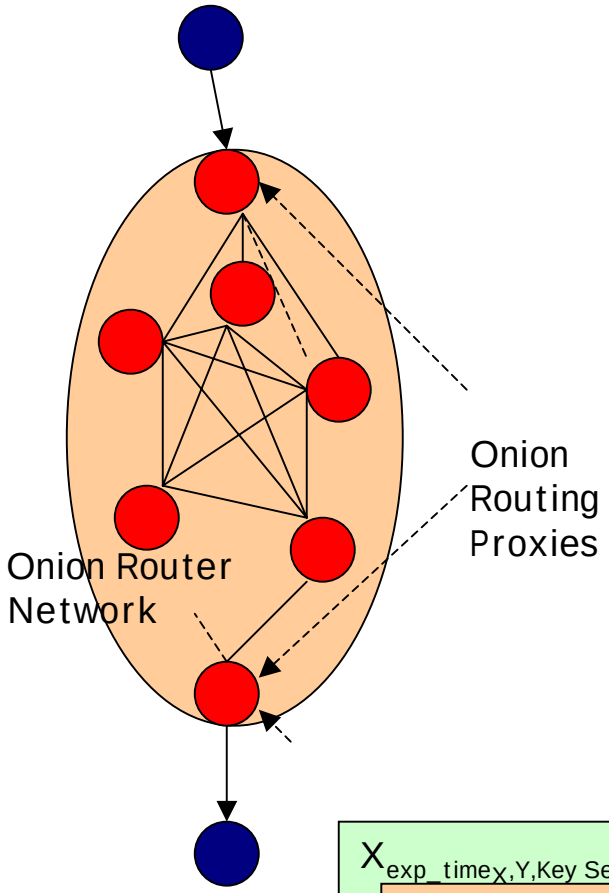


Crowds

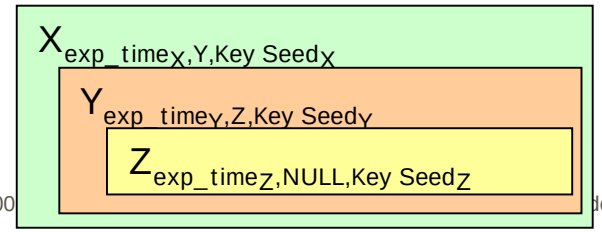


- 1997 von Michael Reiter und Aviel Rubin, AT&T
- Idee: „in der Menge verstecken“
- Zufällige Entscheidung, ob Anfrage zum Zielserver oder an beliebiges anderes Crowd-Mitglied weitergeleitet wird
- symmetrische Verschlüsselung
- Protokolle: http, ftp, gopher, SSL

Onion Routing



- Von David Goldschlag, Michael Reed und Paul Syverson
- MIX-basiertes Verfahren
- Dienste: http, ftp, mail, telnet, finger, whois
- symmetrische Verschlüsselung für Übertragung
- asymmetrische Verschlüsselung



Privacy Management

Infomediaries

P3P

Privacy Management: Ziele

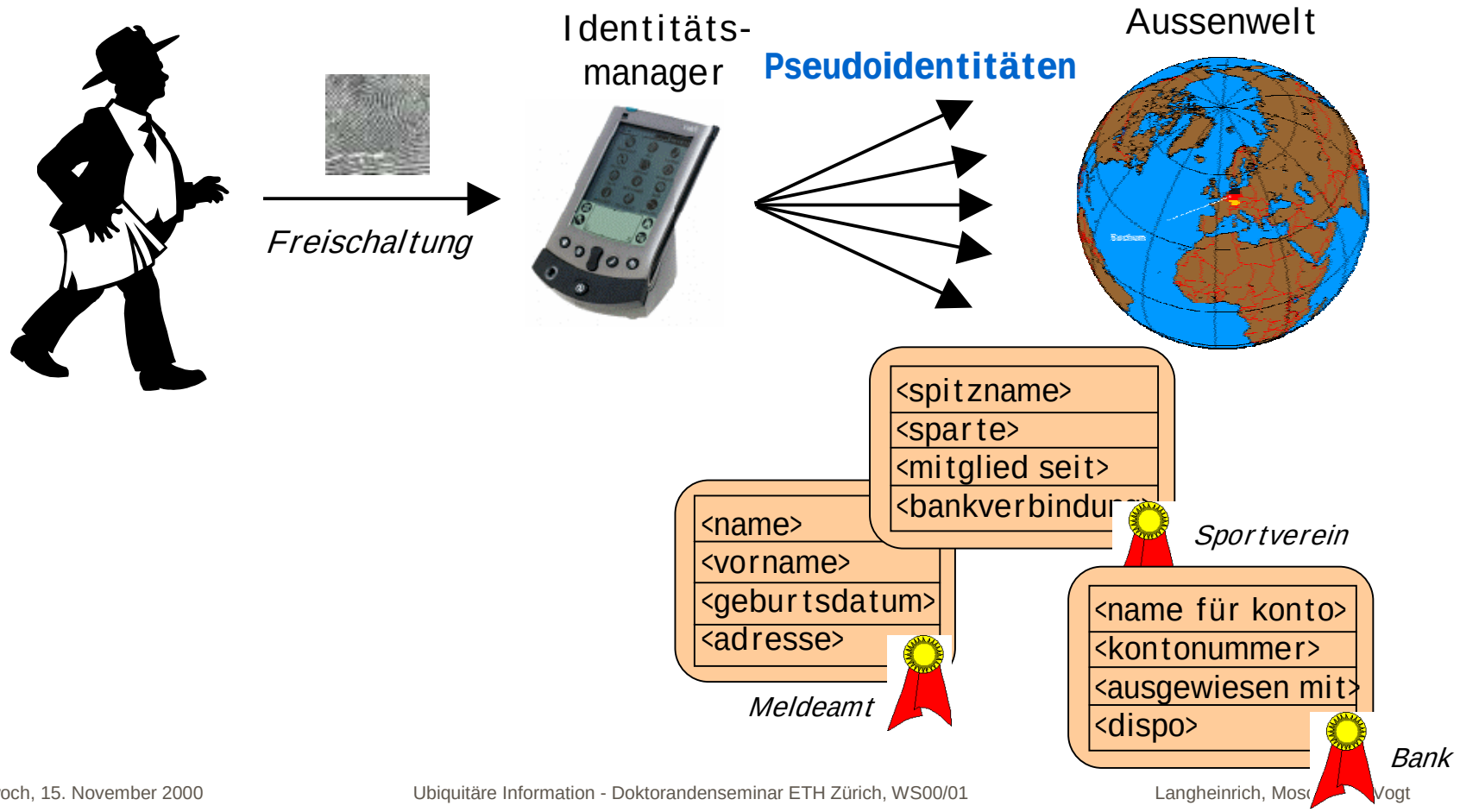
- Kontrolle
  - **Wem** gebe ich **unter welchen Umständen** meine (pseudonymisierten) Daten?
- Transparenz
  - **Wofür** werden diese Informationen benötigt, und **wie** werden sie verwendet?
- Protokollierung
  - **Nachträgliche** Übersicht möglich

Infomediaries

- Bieten Software und Services an
  - Zur Verwaltung von Online-Identitäten (inklusive Passwörtern, e-wallet, etc.)
  - Zur Beurteilung von Datenschutzpraktiken einzelner Websites
  - Zum vereinfachten Ausfüllen von Formularen
- Motto: „Get paid for who you are“
- Finanzierung über
  - Werbung (in der Toolbar eingeblendet)
  - Gebühren von Händlern/Anbietern, die „echte“ Daten wollen

Idee: Identity Protector

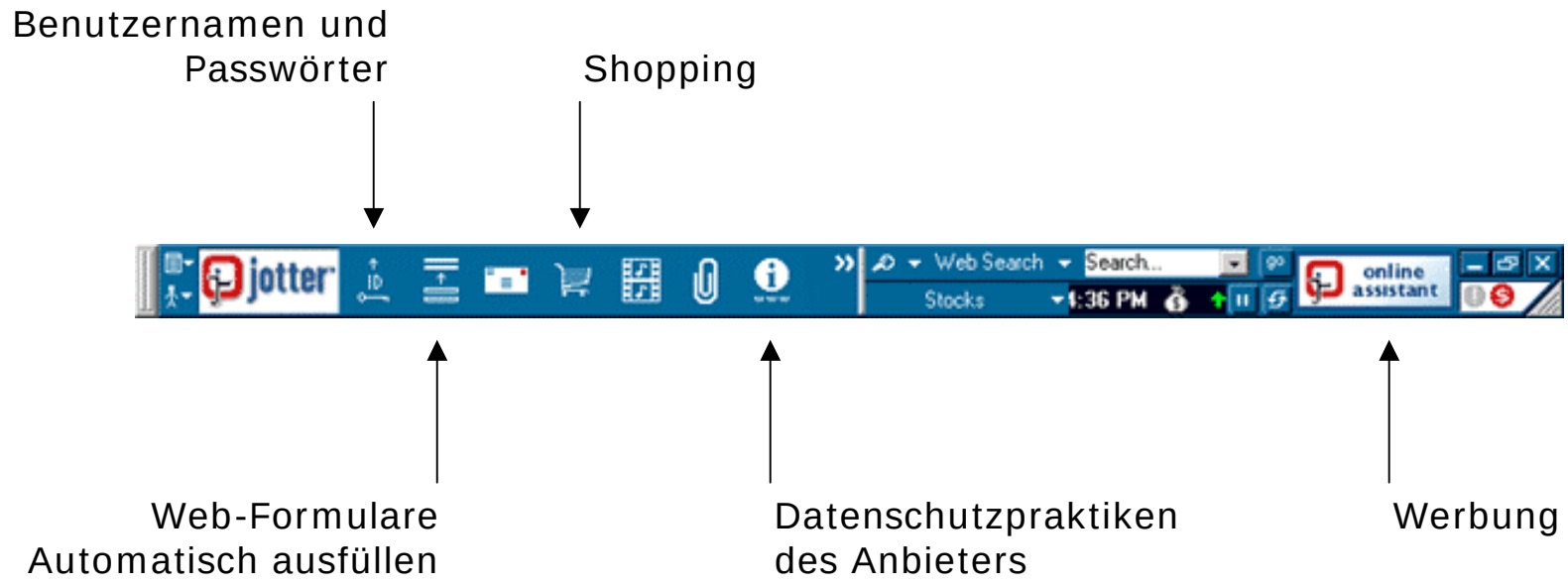
- Konzept von John Borking (1996)



Infomediaries - Beispiele

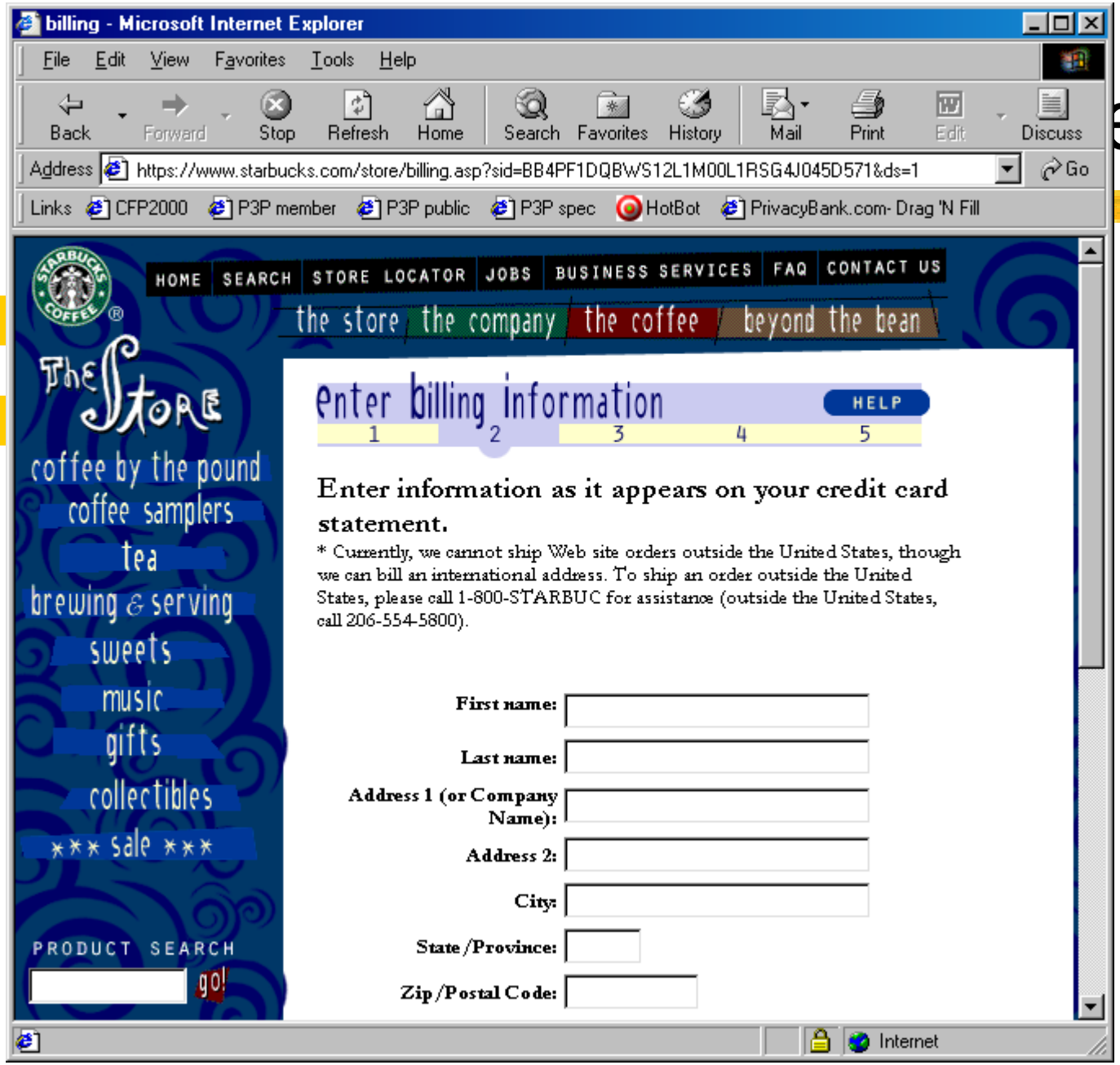
Jotter-Toolbar

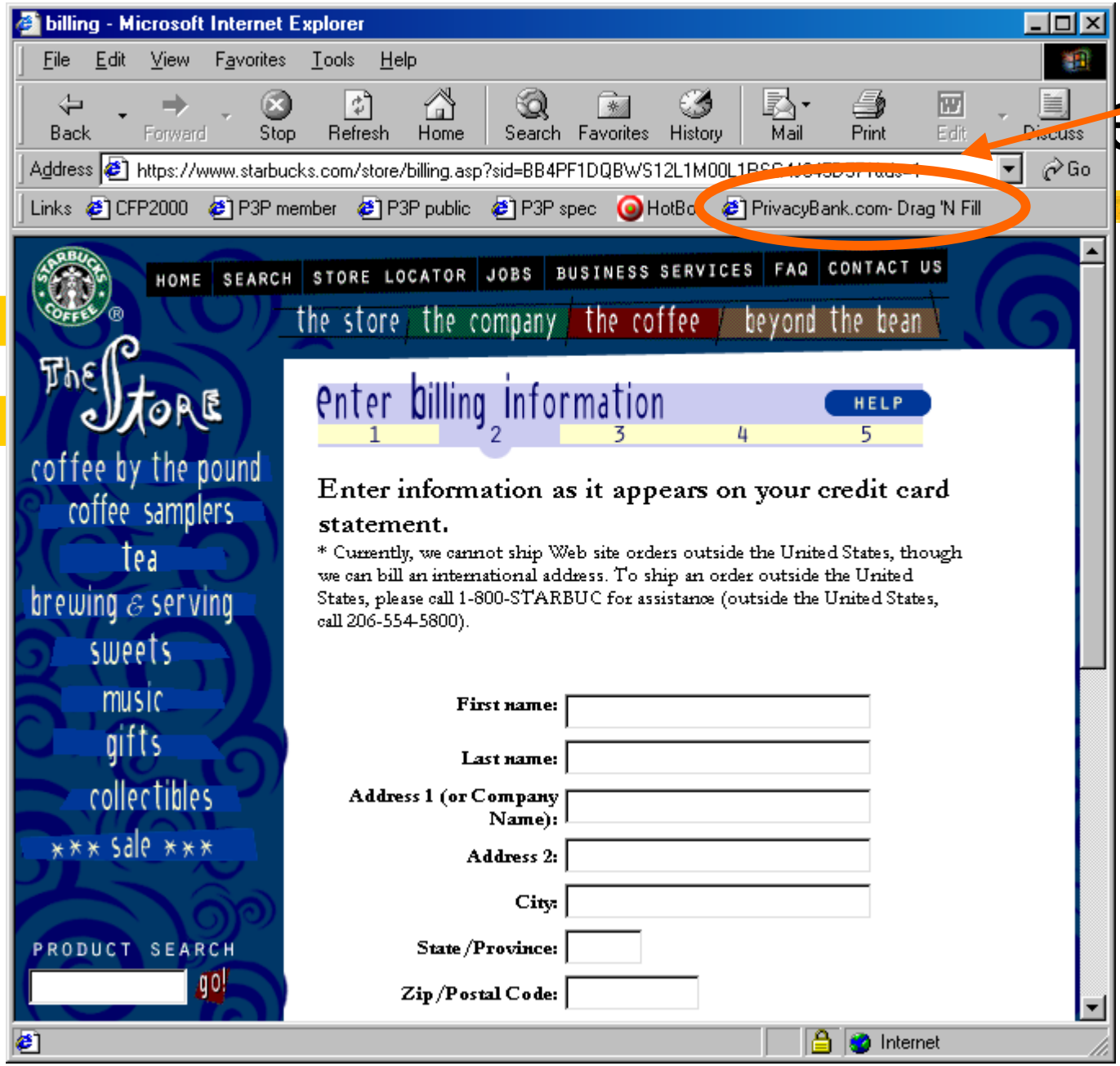
jotter technologies inc.



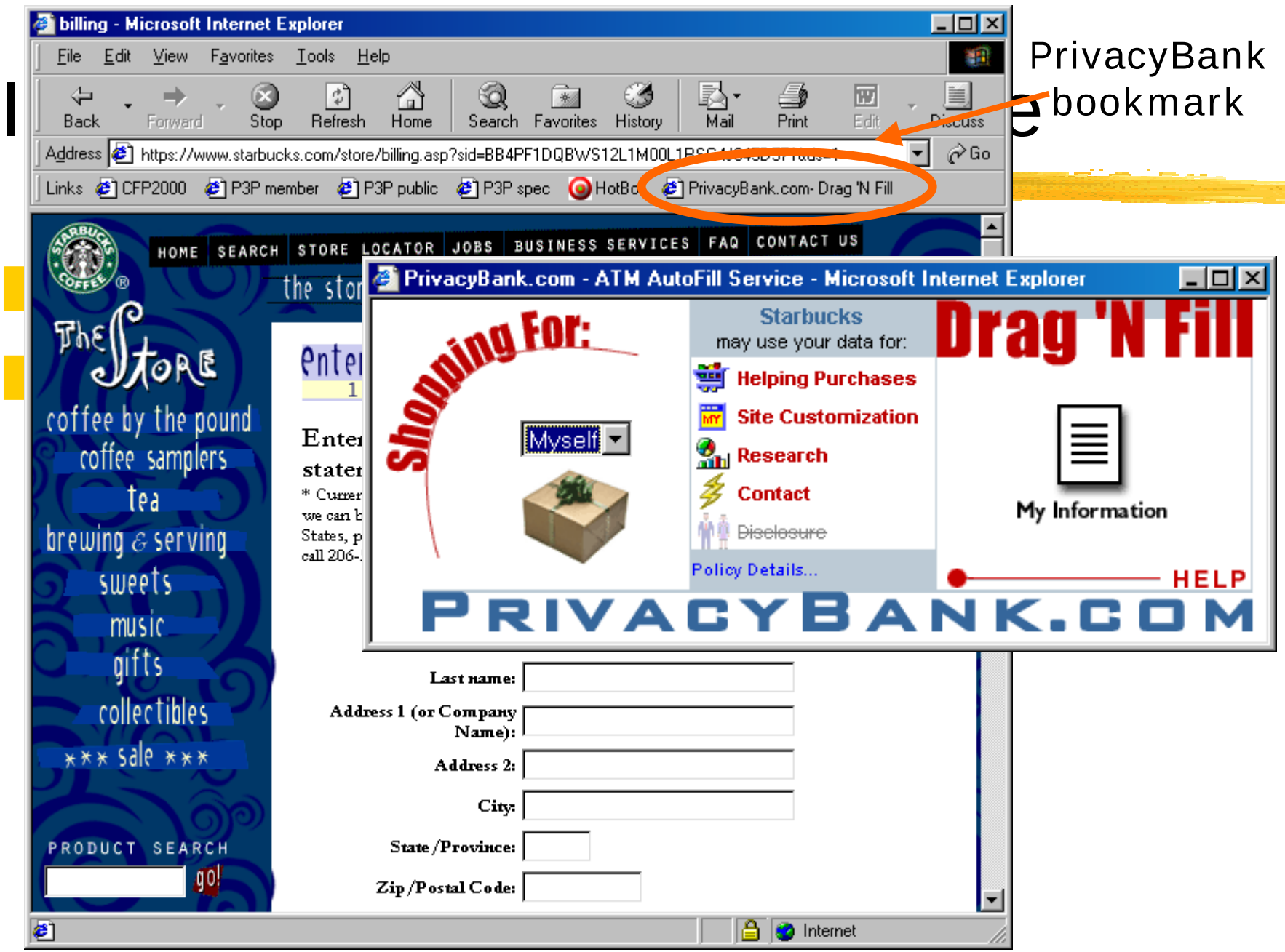
Infomediaries - Beispiele

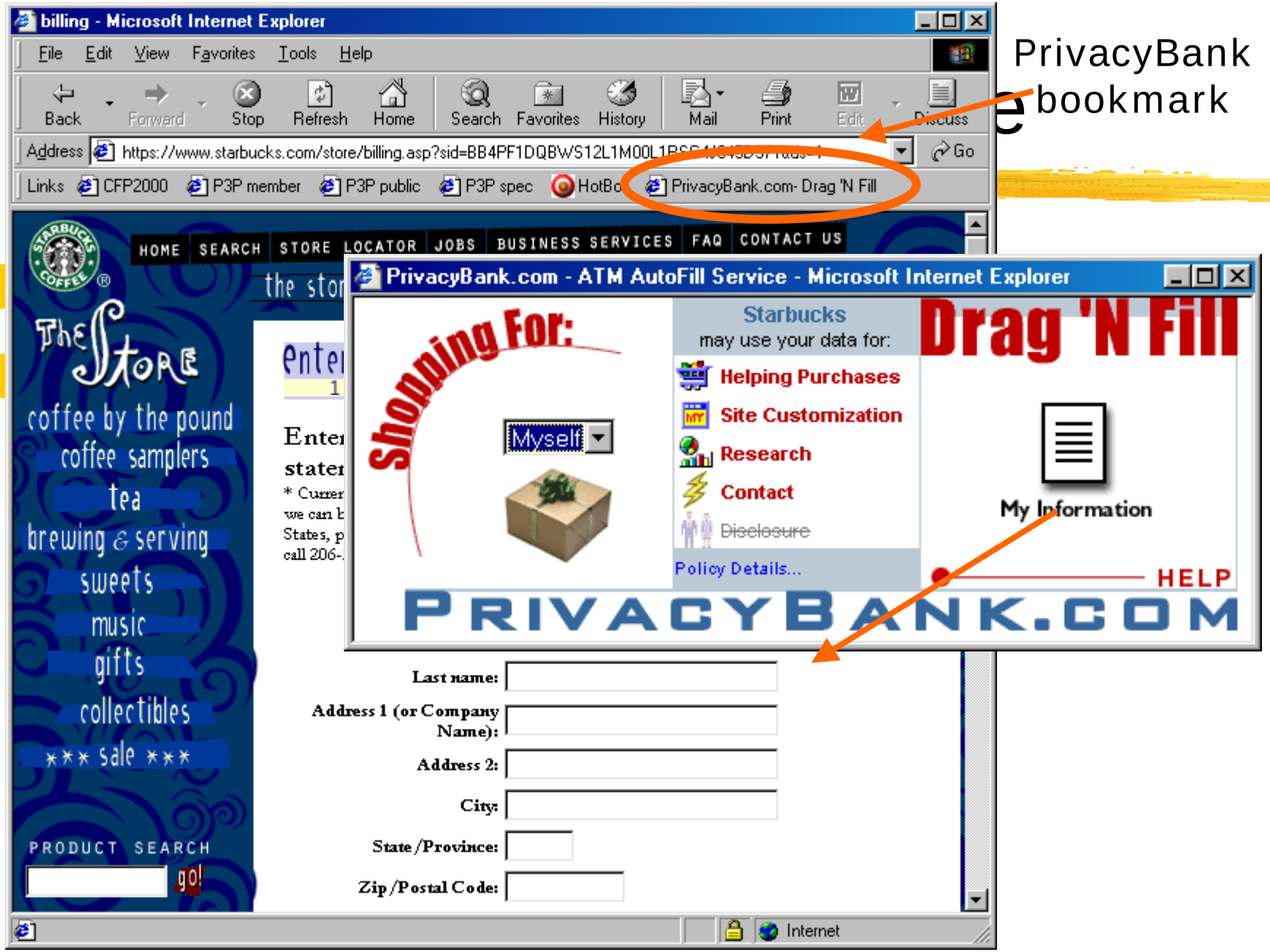
- PrivacyBank.Com
- Bookmark ermöglicht Zugriff auf
  - Datenschutzpraktiken
  - Automatisches Form-Fill-Out


billing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address https://www.starbucks.com/store/billing.asp?sid=BB4PF1DQBWS12L1M00L1RSG4J045D571&ds=1
Go
Links CFP2000 P3P member P3P public P3P spec HotBot PrivacyBank.com- Drag 'N Fill
HOME SEARCH STORE LOCATOR JOBS BUSINESS SERVICES FAQ CONTACT US
the store the company the coffee beyond the bean
The Store
coffee by the pound
coffee samplers
tea
brewing & serving
sweets
music
gifts
collectibles
*** sale ***
PRODUCT SEARCH
go!
enter billing information
HELP
1 2 3 4 5
Enter information as it appears on your credit card statement.
* Currently, we cannot ship Web site orders outside the United States, though we can bill an international address. To ship an order outside the United States, please call 1-800-STARBUC for assistance (outside the United States, call 206-554-5800).
First name:
Last name:
Address 1 (or Company Name):
Address 2:
City:
State/Province:
Zip/Postal Code:
Internet

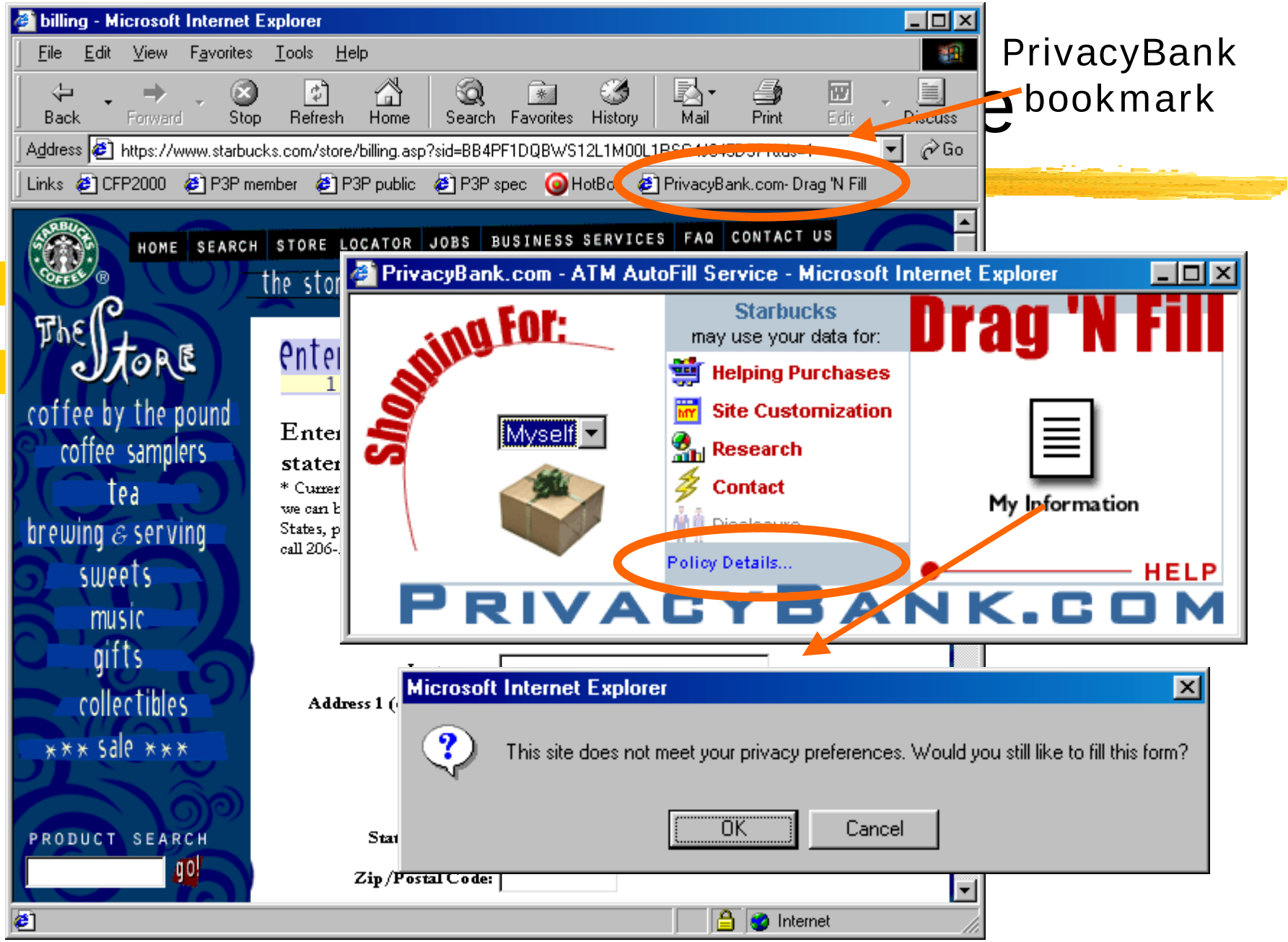


PrivacyBank bookmark


billing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address https://www.starbucks.com/store/billing.asp?sid=BB4PF1DQBWS12L1M00L1
Go
Links CFP2000 P3P member P3P public P3P spec HotBo PrivacyBank.com- Drag 'N Fill
PrivacyBank bookmark
HOME SEARCH STORE LOCATOR JOBS BUSINESS SERVICES FAQ CONTACT US
The Store
coffee by the pound
coffee samplers
tea
brewing & serving
sweets
music
gifts
collectibles
*** sale ***
PRODUCT SEARCH
go!
PrivacyBank.com - ATM AutoFill Service - Microsoft Internet Explorer
Shopping For:
Myself
Starbucks
may use your data for:
Helping Purchases
Site Customization
Research
Contact
Disclosure
Policy Details...
Drag 'N Fill
My Information
HELP
PRIVACYBANK.COM
Last name:
Address 1 (or Company Name):
Address 2:
City:
State/Province:
Zip/Postal Code:
Internet


billing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address https://www.starbucks.com/store/billing.asp?sid=BB4PF1DQBWS12L1M00L1
Go
Links CFP2000 P3P member P3P public P3P spec HotBo PrivacyBank.com- Drag 'N Fill
HOME SEARCH STORE LOCATOR JOBS BUSINESS SERVICES FAQ CONTACT US
The Store
coffee by the pound
coffee samplers
tea
brewing & serving
sweets
music
gifts
collectibles
*** sale ***
PRODUCT SEARCH
go!
PrivacyBank.com - ATM AutoFill Service - Microsoft Internet Explorer
Shopping For:
Myself
Starbucks
may use your data for:
Helping Purchases
Site Customization
Research
Contact
Disclosure
Policy Details...
Drag 'N Fill
My Information
HELP
PRIVACYBANK.COM
Last name:
Address 1 (or Company Name):
Address 2:
City:
State/Province:
Zip/Postal Code:
Internet
PrivacyBank bookmark


billing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address https://www.starbucks.com/store/billing.asp?sid=BB4PF1DQBWS12L1M00L1
Links CFP2000 P3P member P3P public P3P spec HotBo PrivacyBank.com- Drag 'N Fill
PrivacyBank bookmark
HOME SEARCH STORE LOCATOR JOBS BUSINESS SERVICES FAQ CONTACT US
The Store
coffee by the pound
coffee samplers
tea
brewing & serving
sweets
music
gifts
collectibles
*** sale ***
PRODUCT SEARCH
go!
PrivacyBank.com - ATM AutoFill Service - Microsoft Internet Explorer
Shopping For:
Myself
Starbucks
may use your data for:
Helping Purchases
Site Customization
Research
Contact
Disclosure
Policy Details...
Drag 'N Fill
My Information
HELP
PRIVACYBANK.COM
Address 1 (
Zip/Postal Code:
Microsoft Internet Explorer
This site does not meet your privacy preferences. Would you still like to fill this form?
OK
Cancel
Internet


billing - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address https://www.starbucks.com/store/billing.asp?sid=BB4PF1DQBWS12L1M00L1
Links CFP2000 P3P member P3P public P3P spec HotBo PrivacyBank.com- Drag 'N Fill
PrivacyBank bookmark
HOME SEARCH STORE LOCATOR JOBS BUSINESS SERVICES FAQ CONTACT US
The Store
coffee by the pound
coffee samplers
tea
brewing & serving
sweets
music
gifts
collectibles
*** sale ***
PRODUCT SEARCH
go!
PrivacyBank.com - ATM AutoFill Service - Microsoft Internet Explorer
Shopping For:
Myself
Starbucks
may use your data for:
Helping Purchases
Site Customization
Research
Contact
Policy Details...
Drag 'N Fill
My Information
HELP
PRIVACYBANK.COM
Address 1 (
Zip/Postal Code:
Microsoft Internet Explorer
This site does not meet your privacy preferences. Would you still like to fill this form?
OK
Cancel
Internet

Infomediaries – Lohnendes Geschäft?

- Jotter – www.jotter.com
- PrivacyBank.com – www.privacybank.com
- Digitalme – www.digitalme.com
- Lumeria – www.lumeria.com
- Privaseek – www.privaseek.com
- @yourcommand – www.yourcommand.com
- InterOmni – www.interomni.com
- Novell – www.digitalme.com

Privacy Management: Ziele

- Kontrolle
  - **Wem** gebe ich **unter welchen Umständen** meine (pseudonymisierten) Daten?

Transparenz

Wofür werden diese Informationen benötigt, und **wie** werden sie verwendet?

- Protokollierung
  - **Nachträgliche** Übersicht möglich

Platform for Privacy Preferences Project (P3P)

- Projekt am World Wide Web Consortium (W3C)
- Eigentliches Ziel (August 1997):
  - Web Sites bieten Datenschutzpraktiken („privacy policy“) in maschinenlesbarer Form an
  - Web Browser lesen diese automatisch und vergleichen sie mit Präferenzen des Benutzers
  - ~~Web Site und Browser können dann über Praktiken verhandeln~~

Platform for Privacy Preferences Project (P3P)

- Projekt am World Wide Web Consortium (W3C)
- Eigentliches Ziel (August 1997):
  - Web Sites bieten Datenschutzpraktiken („privacy policy“) in maschinenlesbarer Form an
  - Web Browser lesen diese automatisch und vergleichen sie mit Präferenzen des Benutzers
  - ~~Web Site und Browser können dann über Praktiken verhandeln~~
- Erste stabile Version: P3P1.0 (November 2000)
  - Keine Verhandlung (automatisch oder manuell)

P3P1.0 definiert...

- Standard Schemata (**Welche** Daten werden erhoben)
  - `User.name.given`, `User.name.family`, etc.
- Vokabular für Datenschutzpraktiken (**Warum** werden Daten erhoben, **Wie**, etc)
  - `Purpose=marketing`, `Recipient=ourselves`, etc.
- XML Format zum Ausdruck von Datenschutzpraktiken (maschinenlesbar)
- Referenz-Syntax zur Assoziation von Praktiken mit einzelnen Web Seiten oder Sites
- Transportmechanismus für DS-Praktiken (via HTTP)

P3P1.0 definiert...

- Standard
  - User.
- Vokabula
  Daten er
  - Purpo
- XML For
  (maschin
- Referenz
  einzelner
- Transpor

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
     <CONSEQUENCE-GROUP>
       <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
     </CONSEQUENCE-GROUP>
     <RECIPIENT><ours/></RECIPIENT>
     <RETENTION><indefinitely/></RETENTION>
     <PURPOSE><custom/><develop/></PURPOSE>
     <DATA-GROUP>
       <DATA name="dynamic.cookies" category="state"/>
       <DATA name="dynamic.miscdata" category="preference"/>
       <DATA name="user.gender"/>
       <DATA name="user.home." optional="yes"/>
     </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
     <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

P3P1.0 definiert...

- Standard
  - User.
- Vokabula
  Daten er
  - Purpo
- XML For
  (maschin
- Referenz
  einzelner
- Transpor

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="“TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
     <CONSEQUENCE-GROUP>
        <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
      </CONSEQUENCE-GROUP>
     <RECIPIENT><ours/></RECIPIENT>
      <RETENTION><indefinitely/></RETENTION>
     <PURPOSE><custom/><develop/></PURPOSE>
     <DATA-GROUP>
       <DATA name="dynamic.cookies" category="state"/>
       <DATA name="dynamic.miscdata" category="preference"/>
       <DATA name="user.gender"/>
       <DATA name="user.home." optional="yes"/>
     </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
     <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

P3P1.0 definiert...

- Standard
  - User.
- Vokabula
  Daten er
  - Purpo
- XML For
  (maschin
- Referenz
  einzelner
- Transpor

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
     <CONSEQUENCE-GROUP>
        <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
      </CONSEQUENCE-GROUP>
     <RECIPIENT><ours/></RECIPIENT>
      <RETENTION><indefinitely/></RETENTION>
     <PURPOSE><custom/><develop/></PURPOSE>
     <DATA-GROUP>
       <DATA name="dynamic.cookies" category="state"/>
       <DATA name="dynamic.miscdata" category="preference"/>
       <DATA name="user.gender"/>
       <DATA name="user.home." optional="yes"/>
     </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
     <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

P3P1.0 definiert...

- Standard
  - User.
- Vokabula
  Daten er
  - Purpo
- XML For
  (maschin
- Referenz
  einzelner
- Transpor

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
<STATEMENT>
   <CONSEQUENCE-GROUP>
      <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
    </CONSEQUENCE-GROUP>
   <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
   <PURPOSE><custom/><develop/></PURPOSE>
   <DATA-GROUP>
     <DATA name="dynamic.cookies" category="state"/>
     <DATA name="dynamic.miscdata" category="preference"/>
     <DATA name="user.gender"/>
     <DATA name="user.home." optional="yes"/>
   </DATA-GROUP>
</STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
     <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

P3P1.0 definiert...

- Standard
  - User.
- Vokabula
  Daten er
  - Purpo
- XML For
  (maschin
- Referenz
  einzelner
- Transpor

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
     <CONSEQUENCE-GROUP>
       <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
     </CONSEQUENCE-GROUP>
     <RECIPIENT><ours/></RECIPIENT>
     <RETENTION><indefinitely/></RETENTION>
     <PURPOSE><custom/><develop/></PURPOSE>
     <DATA-GROUP>
       <DATA name="dynamic.cookies" category="state"/>
       <DATA name="dynamic.miscdata" category="preference"/>
       <DATA name="user.gender"/>
       <DATA name="user.home." optional="yes"/>
     </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
     <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

P3P1.0 definiert...

- Standard
  - User.r
- Vokabula
  Daten erh
  - Purpos
- XML Forn
  (maschin
- Referenz-
  einzelnen
- Transport

```
<POLICY-REFERENCES
  xmlns="http://www.w3.org/2000/P3Pv1"
  xmlns:web="http://www.w3.org/1999/02/22-rdf-syntax-ns#" >
 <web:RDF>

 <POLICY-REF web:about="/P3P/Policy1.xml">
   <PREFIX>/</PREFIX>
   <EXCLUDE>/catalog/</EXCLUDE>
   <EXCLUDE>/cgi-bin/</EXCLUDE>
   <EXCLUDE>/servlet/</EXCLUDE>
 </POLICY-REF>

 <POLICY-REF web:about="/P3P/Policy2.xml">
   <PREFIX>/catalog/</PREFIX>
 </POLICY-REF>

 </web:RDF>
</POLICY-REFERENCES>
```

P3P1.0 definiert...

- Standard Schemata (**Welche** Daten werden erhoben)
  - `User.name.given`, `User.name.family`, etc.
- Vokabular für Datenschutzpraktiken (**Warum** werden Daten erhoben, **Wie**, etc)
  - `Purpose=marketing`, `Recipient=ourselves`, etc.
- XML Format zum Ausdruck von Datenschutzpraktiken (maschinenlesbar)
- Referenz-Syntax zur Assoziation von Praktiken mit einzelnen Web Seiten oder Sites
- Transportmechanismus für DS-Praktiken (via HTTP)

Browsing ohne P3P1.0

Web Server

GET /x.html HTTP/1.1

. . . Request web page

HTTP/1.1 200 OK
Content-Type: text/html

. . . Send web page

Browsing mit P3P1.0

Web Server

GET /p3p.xml HTTP/1.1
. . . Request Policy Reference File

Send Policy Reference File

Request P3P Policy

Send P3P Policy

GET /x.html HTTP/1.1
. . . Request web page

HTTP/1.1 200 OK
Content-Type: text/html
. . . Send web page

Status von P3P

- Mitarbeit von Industrie, Regierung und Datenschützer
  - AOL/Netscape, Microsoft, IBM, EU (Arbeitsgruppe für Datenschutzgesetze), DSB Hong Kong, Canada, Niederlande, Deutschland, ...
- Prototyp Implementationen von
  - Microsoft, IBM, AT&T, ...
- Mehrer Web Sites bereits P3P-fähig
  - www.whitehouse.gov, www.hp.com, www.microsoft.com, www.ibm.com, ...

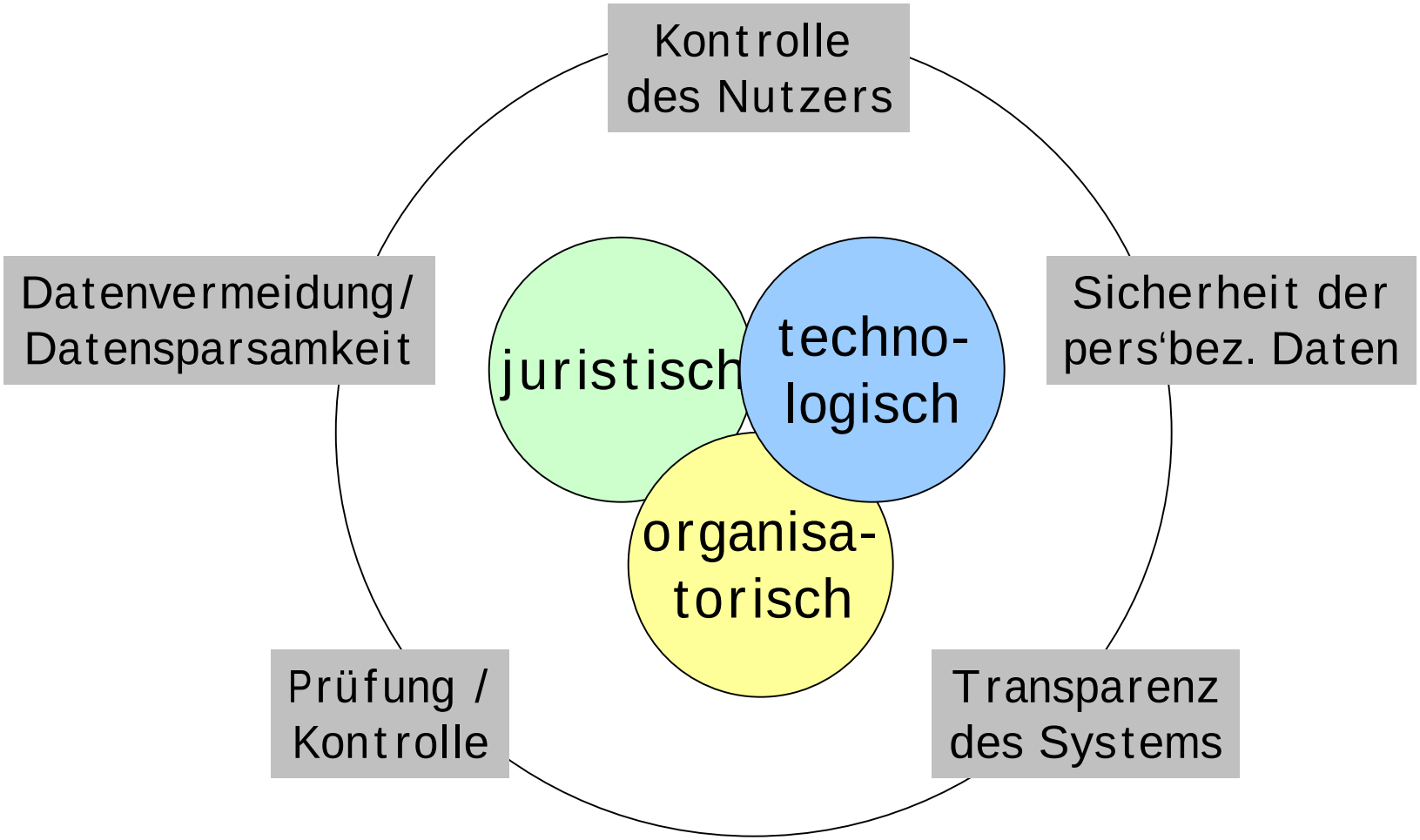
P3P ist *Teil* einer Lösung

- Ermöglicht Transparenz bei Datenschutz-Praktiken
- Benötigt aber auch:
  - Anonymisierungs-Werkzeuge
  - Verschlüsselungs-Software
  - Rechtliche Werkzeuge (wer garantiert, dass sich Anbieter an ihre Praktiken halten?!)

Soziale Kontrolle

Datenschutzgesetz
Betreibermassnahmen

Datenschutzanforderungen an die Technikgestaltung



Europarecht

- „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr“ (24.10.1995)
- Inhalt:
  - Aufhebung der Trennung zwischen öffentlichem und nicht-öffentlichem Bereich
  - Staatliche Stellen erhalten erweiterte Befugnisse
  - Zweckbindung der Datenerhebung wurde verstärkt
  - Regelung des Exports von personen-bezogenen Daten in das Ausland
  - ...

Europarecht (2)

- Regelung des Exports von personen-bezogenen Daten in das Ausland:
  - EU-Länder: Export erleichtert
  - Nicht-EU-Länder: Export nur zulässig, wenn der Drittstaat angemessenes Schutzniveu gewährleistet
  - Beispiel USA:
    - Konzept „Safe Harbour“: Unternehmen der USA verpflichten sich auf Privacy-Regeln nach dem Vorbild der EU-Richtlinien
    - Überwachung erfolgt durch Unternehmen selbst
    - FTC (Federal Trade Commission) kann wegen Betrugs einschreiten, jedoch nicht auf Betreiben einer Privatperson

Datenschutzgesetze in Deutschland

- Bundesdatenschutzgesetz (BDSG):
  - schützt „**informationelle Selbstbestimmung**“ als vorgelagerten Persönlichkeitsschutz
    - ➔ **grundrechtgleiches Recht**
  - Für die Vorschriften gelten die Grundsätze
    - der Normenklarheit und des Übermassverbots
    - der Zweckbindung: eine gesetzliche Grundlage muss eindeutig den Zweck der Datenverarbeitung festlegen und eingrenzen.
  - Geltungsbereich: öffentlicher, staatlicher Bereich und nicht-öffentlicher Bereich

Datenschutzgesetze in Deutschland (2)

- Landesdatenschutzgesetze:
  - Geltungsbereich: innere Verwaltung des Landes
- Datenschutz im Betrieb:
  - kein eigenständiges betriebliches Datenschutzrecht
  - Es besteht Einigkeit darüber, dass:
    - Arbeitnehmerdaten nur zu bestimmten Zwecken erhoben werden dürfen
    - Betriebsrat hat Verpflichtung und Kompetenz zur Überwachung der Einhaltung datenschutzrechtlicher Bestimmungen
    - **Betriebsrat hat Mitbestimmungsrecht bei der Einführung einer technischen Einrichtung** (z.B. Überwachungseinrichtung)

Datenschutzgesetze in Deutschland (3)

- Teledienste-Datenschutzgesetz (TDDSG):
  - Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit dies durch das TDDSG oder anderen Rechtsvorschriften gedeckt ist
  - **Grundsätze**: Datenvermeidung, Zweckbindung, Systemschutz
  - Bestandsdaten dürfen auf Ersuchen staatlicher Stellen zur Verfolgung von Straftaten weitergegeben werden
  - Unentgeltliches Einsichtsrecht in eigene Daten
  - ...

Datenschutzgesetze - Beispiel Videoüberwachung

Öffentlicher Bereich:

- Kriminalitätsschwerpunkte, Verkehrsbetriebe, Schulen, Krankenhäuser,...

Nicht-öffentlicher Bereich:

- Kaufhäuser, Supermärkte, Tankstellen, Banken, Deutsche Bahn,...
- Wohnumfeld
- Arbeitsverhältnis
- Webcams

Datenschutzgesetze - Beispiel Videoüberwachung

Öffentlicher Bereich:

- Kriminalitätsschwerpunkte, Verkehrsbetriebe, Schulen, Krankenhäuser,…

  Verhinderung, Verfolgung von Straftaten und Ordnungswidrigkeiten, Reduzierung von Vandalismusschäden

Zweckbindung

Nicht-öffentlicher Bereich:

- Kaufhäuser, Supermärkte, Tankstellen, Banken, Deutsche Bahn,…

  Verhinderung, Verfolgung von Straftaten und Ordnungswidrigkeiten, Reduzierung von Vandalismusschäden
- Wohnumfeld

  Verbesserung der Wohnqualität
- Arbeitsverhältnis
- *Warenverlust*
- Webcams

  KEINE Zweckbindung!!

Datenschutzgesetze - Beispiel Videoüberwachung

Öffentlicher Bereich:

•Kriminalitätsschwerpunkte, Verkehrsbetriebe, Schulen, Krankenhäuser,…

Verhinderung, Verfolgung von Straftaten und Ordnungswidrigkeiten, Reduzierung von Vandalismusschäden

Zweckbindung

Rechtsgrundlage

- **Untersuchung einer (konkreten) Straftat**
- **Verhütung von Straftaten**
- **Abwehr von Gefahr**
- **Gefahr für die öffentliche Sicherheit**

Nicht-öffentlicher Bereich:

•Kaufhäuser, Supermärkte, Tankstellen, Banken, Deutsche Bahn,…

Verhinderung, Verfolgung von Straftaten und Ordnungswidrigkeiten, Reduzierung von Vandalismusschäden

•Wohnumfeld

Verbesserung der Wohnqualität

•Arbeitsverhältnis

• *Warenverlust*

•Webcams

KEINE Zweckbindung!!

- **Für den Einsatz von Videotechnik durch Privatunternehmen und -personen fehlt jegliche rechtliche Regelung**

Datenschutzgesetze - Beispiel Videoüberwachung II

- Datenschutzgesetze ermöglichen KEINE Entscheidung über die Zulässigkeit des Einsatzes der Videotechnik
- Regelungsprinzipien:
  - dient die Videotechnik lediglich der Beobachtung von Räumen, die ebenso gut von einem Menschen beobachtet werden könnte, ist der Einsatz zulässig, soweit er ***im Rahmen der Arbeitserfüllung, der Vertragsabwicklung oder der Wahrnehmung des Hausrechts*** angemessen ist.
  - Da eine Videoüberwachung einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte darstellen würde, ist ***über den Kameraeinsatz zu informieren***.
  - ***Aufzeichnung***: … nur dann zulässig, wenn eine Straftat beobachtet wird oder eine konkrete Gefahrenlage besteht.

Technischer Datenschutz

- Personenbezogene Daten dürfen verarbeitet werden, soweit dies **gesetzlich zugelassen** oder von eine **Einwilligung** gedeckt ist
- Bester Datenschutz: keine oder möglichst wenig personenbezogene Daten
  - → **Datenvermeidung** und **Datensparsamkeit**
  - → **Verwendungsmöglichkeit einschränken und Zweckbindung gewährleisten**

→ **Anonymitäts- und Pseudonymitätsverfahren**

Technischer Datenschutz

Vertraulichkeit

- Unnötige Daten vermeiden
- Verwendungsmöglichkeit notwendiger Daten einschränken
- Verwendung notwendiger Daten einschränken

Korrektheit

- Überprüfung der Daten durch Betroffenen bei jeder Verwendung
- Überprüfung der Daten durch Betroffenen

Vertraulichkeit

- starke Massnahmen:
  - keine Datenerfassung
- mittlere Massnahmen:
  - Transaktionspseudonyme
  - Rollenpseudonyme
  - Personenpseudonyme
  - dig. Pseudonyme
- schwache Massnahmen:
  - verteilte Speicherung
  - Protokollierung
  - Organisation
  - Vorschriften

Korrektheit

- mittlere Massnahmen:
  - Betroffener online + digitale Signaturen
- schwache Massnahmen:
  - mobiles Datenverarbeitungssystem
  - bei jeder Verwendung Mitteilung an Betroffenen
  - abfragbare Log-Files
  - Auskunftsrecht

Privacy und Ubicomp

- Zusätzliche Gefahren im Ubicomp
- Generelle Bedrohungen
- Diskussion

Ubicomp-Besonderheiten

- Benutzerschnittstellen
  - Fehleranfälligkeit
  - Natürliche Sprache abhörbar
- Verborgenheit
  - Rechner sind allgegenwärtig, aber „unsichtbar“
  - Fehlende Rückmeldung
  - Mangelndes Bewusstsein

Bedrohungen

- Identity theft
  - 1999: 39‘000 Fälle von SSN-Missbrauch
- Denial of service
  - Abhängigkeit von Systemen nimmt zu, etwa durch Angriffe auf Server *und* Klienten
  - Administrationsschwächen
- Gegenseitige Abhängigkeit
  - Zunehmende Vernetzung untereinander
  - Jeder weiss mehr über den anderen

Diskussion

- Mehr Technik, mehr Fehler
- Zunehmende Abhängigkeit von Systemen
  - Gefährdung der Privacy nimmt zu
- Neue Bedrohungen...
  - erfordern neue Gegenmassnahmen
  - Anwendbarkeit herkömmlicher Techniken?
  - Einfache Techniken notwendig
- Besserer Datenschutz durch Ubicomp?

Die Zukunft sieht düster aus

- **Standards** benötigen immer längerere Entwicklungszeiten und werden entweder „aufgeweicht“ oder in konkurrierende Systeme zersplittert
- **Gesetze** können nicht mehr mit aktueller Entwicklung mithalten (Napster, Explorer, aber auch Patente)
- Statt Gerichten entscheiden Internetfirmen über **Streitfälle** (Alternative Dispute Resolution Mechanism, Internic)
- Technologien und Geräte werden immer komplizierter und unüberschaubarer – **Kontrolle** für den Benutzer geht verloren
- Technologie kann helfen, stösst aber auf Ablehnung beim Verbraucher (**Technikfeindlichkeit**)
- **Kommerz** contra Verbraucherschutz, letzerer muss sich dem „Wohlstand“ unterordnen
- => Privacy geht unwiederbringlich verloren

Die Zukunft sieht rosig aus!

- **Standards** werden internationaler – keine Alleingänge mehr möglich
- Wirkungsvolle **Gesetze** zum Schutz des Verbrauchers werden International akzeptiert (EU Direktive -> Safe Harbor)
- Gütesiegel-Programme bieten effektiven Schutz und Hilfe, auch in Abwesenheit von Gesetzen
- Technologien und Geräte werden durch Ubicomp einfacher! Der Benutzer erhält die **Kontrolle** zurück
- Technologie erlaubt wirkungsvollen Schutz vor Identifikation und Abhören, ermöglicht aber auch anonyme Authentisierung
- **Kommerz** sieht Verbraucherschutz als Verkaufsargument!
- => Kontrolle über persönliche Daten ist mehr denn je in den Händen der Verbraucher (Privacy Management Tools)