

Privacy in Ubiquitous Computing

Dagstuhl Retreat
September 13, 2001

Marc Langheinrich
ETH Zurich

www.inf.ethz.ch/~langhein/

Contents

Dagstuhl Retreat – September 13, 2001

- Why should someone bother?
 - 10 Facts about Privacy
- Why should *I* bother?
 - 5 Reasons why Ubicomp People must work harder
- What can one do about it?
 - 10 Steps to Privacy (+ Requirements)
 - Transparency Tools

1. A Human Right

Dagstuhl Retreat – September 13, 2001

- 1948 United Nations, Universal Declaration of Human Rights: Article 12
 - No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks
- 1970 European Convention on Human Rights: Article 8 – Right to respect for private and family life
 - Everyone has the right to respect for his private and family life, his home and his correspondence. ...

(Long History)

Dagstuhl Retreat – September 13, 2001

- Bible, Jewish Law („...free from being watched“)
- Justices of the Peace Act (England, 1361)
- „The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement“
(William Pitt, English Parliamentarian, 1765)
- „Right to be left alone“ (Brandeis & Warren, 1890)

2. A Legal Requirement

Dagstuhl Retreat – September 13, 2001

- Privacy laws and regulations vary widely throughout the world
- US has mostly sector-specific laws, with relatively minimal protections
 - Government has comprehensive “Privacy Act” (1974)
 - Industry favors Self-Regulation over comprehensive Privacy Laws, says regulation hinders e-commerce
- Europe has long favored strong privacy laws
 - First data protection law in the world: State of Hesse, Germany (1970)
 - Privacy commissions in each country (some countries have national and state commissions)

(Some US Privacy Laws)

Dagstuhl Retreat – September 13, 2001

- Bank Secrecy Act, 1970
- Fair Credit Reporting Act, 1971
- Privacy Act, 1974
- Right to Financial Privacy Act, 1978
- Cable TV Privacy Act, 1984
- Video Privacy Protection Act, 1988
- Family Educational Right to Privacy Act, 1993
- Electronic Communications Privacy Act, 1994
- Freedom of Information Act, 1966, 1991, 1996

- Recent Additions: HIPAA, COPPA, GLBA

(EU Data Directive)

Dagstuhl Retreat – September 13, 2001

- 1995 Data Protection Directive 95/46/EC
 - sets a benchmark for national law for processing personal information in electronic and manual files
 - facilitates data-flow between member states and restricts export of personal data to „unsafe“ non-EU countries
- 1997 Telecommunications Directive
 - establishes specific protections covering telecommunications systems
 - July 2000 proposal to strengthen and extend directive to cover „electronic communications“
- Member states responsible for passing relevant national laws by 10/1998
 - 11 out of 15 member states have passed legislation, 4 are still pending (as of 09/2001)

(OECD Fair Information Principles)

Dagstuhl Retreat – September 13, 2001

- Collection limitation (data minimization)
- Openness (Notice)
- Purpose specification
- Use limitation
- Individual participation (consent)
- Data quality (updates)
- Security safeguards
- Accountability

<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM>
09/1980

(Privacy around the World)

Dagstuhl Retreat – September 13, 2001

- Australia*
 - Proposed: Privacy Amendment (Private Sector) Bill in 2000
 - In talks with EU officials
- Brazil
 - Proposed: Bill No. 61 in 1996 (pending)
- Canada*
 - Passed: Bill C-6 in 4/2000
 - Under review by EU
- Hong Kong*
 - Passed: Personal Data (Privacy) Ordinance in 1995
- Japan
 - Currently: self-regulation & prefectural laws
 - In talks with EU officials
- Russia
 - Law on Information, Informatization, and Inform. Protect. 1995
 - In Progress: updated to comply with EU directive
- South Africa
 - Planned: Privacy and Data Protection Bill
- Switzerland*
 - EU-certified safe third country for data transfers

<http://www.privacyinternational.org/survey/>

* Has National Privacy Commissioner

3. Privacy Sells!

Dagstuhl Retreat – September 13, 2001

- 03/1999: IBM shows ads only on Websites with privacy policy
 - 2nd largest Web Advertiser
- 02/2000 DoubleClick announces plans to merge “anonymous” online data with personal information obtained from offline databases
 - Stock dropped from \$125 (12/99) to \$80 (03/00)

4. It's Expensive

Dagstuhl Retreat – September 13, 2001

- 05/2001 Study estimates Cost for Web Privacy Policies:
 - From US \$9 Billion to \$36 Billion (Direct Costs for modifying Web Site and Back-end Systems)
 - Caveat: No off-the-shelf software considered
- Privacy Planning Takes Time & Money
 - Data Collection Planning
 - Data Access Provision
 - ...

5. Ignorance is Expensive

Dagstuhl Retreat – September 13, 2001

- Brand/Reputation Damage
 - Lack of Trust == Loss of Revenue?
 - Japan's Ministry of Postal & Telecomm. Survey, 1999
 - 70% have interest in privacy protection
 - 92% fear that personal information is used unknowingly
- Attorney Costs
- Security Costs
 - Expensive to Store Unnecessary Data

6. It's not just Anonymity

Dagstuhl Retreat – September 13, 2001

- Effective Technical Solutions for Anonymous Communication
 - Mixes, Proxies, e-Cash, ...
- However, many services require or perform some form of identification
 - Customization, Delivery, Cameras, ...
- Pseudonymity can be good substitute
 - Can be thrown away, though often-used Pseudonyms may become valuable
 - Have Pseudonyms a right to privacy?
- Data Mining may find „real“ identity!

7. It's not just Security

Dagstuhl Retreat – September 13, 2001

- Secure Communications
 - Gets my information safely across
- Secure Storage
 - Locks my information safely away

- Usage?
 - What do they do with my data
- Recipients?
 - Who gets my data?
- Retention?
 - How long do they keep my data?

Transparency

8. No 100% Guarantees

Dagstuhl Retreat – September 13, 2001

- Encryption
 - Codes can be broken (CIA, NSA, ...)
- Watermarking
 - (Simple) Data can be copied (manually)
- Human in the Loop
 - Faults can be made
- Goals:
 - Provide Tools to Privacy-Respecting Parties
 - Support Enforcement of Fraud
 - Prevent Accidents

9. Privacy Requires Trust

Dagstuhl Retreat – September 13, 2001

- Trust Infrastructure
 - In Real-World provided by Global Brands
 - In unbound Virtual World, need Trust Networks, Trust Brands, etc.
- Examples on the Internet



10. It's a Trade-off

Dagstuhl Retreat – September 13, 2001

- Convenience vs. Anonymity
 - The more others know about me, the better they can accommodate my preferences
- Personal Liberty vs. Social Utilitarianism
 - Increased Surveillance for apprehending criminals
 - Success Rate vs. Risk of Failure

Summary Slide

Dagstuhl Retreat – September 13, 2001

- 1. A Human Right
- 2. A Legal Requirement
- 3. Privacy Sells!
- 4. It's Expensive
- 5. Ignorance is Expensive
- 6. It's not just Anonymity
- 7. It's not just Security
- 8. No 100% Guarantees
- 9. Privacy Requires Trust
- 10. It's a Trade-off

Contents

Dagstuhl Retreat – September 13, 2001

- Why should someone bother?
 - 10 Facts about Privacy
- Why should *I* bother?
 - 5 Reasons why Ubicomp People must work harder
- What can one do about it?
 - 10 Steps to Privacy (+ Requirements)
 - Transparency Tools

1. It's Inhomogeneous

Dagstuhl Retreat – September 13, 2001

- Web is easy:
 - Single Protocol
 - Single Interaction Model
- Ubicomp is difficult:
 - Multiple Protocols
 - Peer-to-Peer and Client-Server
 - Human to Computer and Computer to Computer Communications

2. It's Invisible

Dagstuhl Retreat – September 13, 2001

- How do I know if I interact with a digital service?
 - fingerprint might be taken without my knowledge
- How do I know if I'm under surveillance?
 - life recorders, room computers, smart coffee cups, etc

3. It's Comprehensive

Dagstuhl Retreat – September 13, 2001

- Web covers a lot of the real-world
 - Preferences (online shopping)
 - Interests & hobbies (chat, news)
 - Location & Address (online tracking)
- Ubicomp *is* the real-world
 - Permeates our Homes, Cars, Offices, Public Places, Playgrounds, etc
 - No switch to turn it off!
 - Constant Surveillance

4. It's Smart

Dagstuhl Retreat – September 13, 2001

- Better Sensors supply more detailed & precise data
- Previously worthless information can contain important clues
 - Context!
- Might know more about us than we do ourselves!

5. Nobody's Watching

Dagstuhl Retreat – September 13, 2001

- Researchers too playful
 - We want to have fun, after all
- Businesses too forgetful
 - Haven't heard this talk yet
- Lawmakers too busy with the Web
 - Difficult enough
- Society too trustful
 - Census, Supermarket Member Cards, Electronic Road Toll, ...

Contents

Dagstuhl Retreat – September 13, 2001

- Why should someone bother?
 - 10 Facts about Privacy
- Why should *I* bother?
 - 5 Reasons why Ubicomp People must work harder
- What can one do about it?
 - 10 Steps to Privacy (+ Requirements)
 - Transparency Tools

Privacy ToDo List

Dagstuhl Retreat – September 13, 2001

1. How much Data do I need?
2. What about Anonymity and Pseudonymity?
3. Announce Data Collection!
4. Offer a Choice!
5. Get User Consent!
6. Keep Personal Data Secure
7. Delete Unneeded Data ASAP
8. Provide Access
9. Be Accountable
10. Collect & Process Data Locally

Technical Requirements

Dagstuhl Retreat – September 13, 2001

- Built-In Locality & Proximity
- Anonymous Protocols
- Pseudonyms (Identity Management)
- Adaptive Security (Low Power)
- Transparency Protocols (Notice, Choice)
- Privacy-aware Backend Systems (Access & Control)
- Trust Infrastructure

Transparency

Dagstuhl Retreat – September 13, 2001

- Internet Today
 - Human-readable Privacy Policies on Web sites (difficult to read)
 - Trust Seals
- Internet Tomorrow
 - Machine-readable Privacy Policies fetched automatically by browser
 - Machine-readable Trust Seals
 - Browser makes decisions based on user preferences (cookies, data exchange, ...)

P3P

Dagstuhl Retreat – September 13, 2001

- Project by the World Wide Web Consortium (W3C)
- Principle:
 - Web Sites offer privacy policies in machine-readable format
 - Web Browser read policies automatically and take action based on user preferences
- Status:
 - Candidate Recommendation (12/2000)
 - 100+ Web sites P3P-enabled (IBM, MS, ...)
 - P3P support in IE6

P3P defines...

Dagstuhl Retreat – September 13, 2001

- Standard Schemas (**What** Data is collected)
 - `user.name.given`, `user.name.family`, etc.
- Vocabulary for privacy practices (**Why** is this data collected, **How**, etc)
 - `Purpose=marketing`, `Recipient=ourselves`, etc.
- XML-Format (machine-readable) for describing Privacy Policies
- Mechanism to associate privacy policies with individual Web pages or sites
- Transport mechanisms für Policies (via HTTP)

P3P defines...

Dagstuhl Retreat – September 13, 2001

What can one do about it?

- Standard
- use
- Vocabulary
- data
- Pur
- XML-Priva
- Mech
- indivi
- Trans

```
<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>
```

Transparency

Dagstuhl Retreat – September 13, 2001

- UbiComp
 - Machine-readable Privacy Policies emitted by Privacy Beacons
 - Policies read by Personal Privacy Assistant (e.g., smart watch, PDA)
 - Preferences, Data Exchange in Foreground or Background
 - Personal Privacy System keeps track
 - Full Access through Web Interface