



Privacy and Data
Technical Requirements Analysis
Breakout Session
Almaden Institute, 2003

Moderator: Joe Hellerstein, Berkeley

Framework for discussion

This grid was used to focus discussion on technical approaches to privacy and on the various potential “users” or “customers” of such technology.



Technical Approaches
(By analogy to Real World)

	Individual	Organization	Government	Society
Legislation (policy)				
Incentives				
Enforcement (mechanisms)				

Discussion

- We proceeded by bringing up illustrative examples
- From the examples, we developed categories of issues/challenges to be faced:
 - Data Use
 - Trust Relationships
 - Transparency
 - Incentives
 - Technology
 - Types of “Users”
 - Education

Limiting *Secondary Use*

- Examples
 - Cameras were placed at traffic lights to detect running red lights. Were later used for detecting speeders as well.
 - Medical records used for epidemiological study reused by an insurance company
- *Requirement*: specification of purpose for which data is collected
- Mechanisms for enforcement of primary use?

Managing Trust Relationships

- Privacy as related to *trust*
 - I trust the party to which I give data.
 - I may accept their policy, and trust them to adhere to it.
 - *Policy adherence* trust can be enforced/checked by mechanisms.
 - I may accept their policy *only* from them; the same policy from another party may be unacceptable to me.
 - This *relationship trust* with the data recipient may be only loosely related to policy adherence.
 - Can a mechanism control data visibility across changes in relationship?
- Change in relationships can occur between data provider and data recipient
 - E.g. recipient participates in merger/acquisition
 - Effects on policy adherence
 - Effects on desirability of relationship.

Transparency

- Of use
 - Use policy should be well-defined and comprehensible
- Of disclosure
 - You should be able to know what information you give out
 - E.g. unclear whether the magstripe on your driver's license has the same info as the text
- Of technology
 - How do I know what info is extracted, and whether it's extracted faithfully?
 - E.g. swiping my driver's license proves I'm >21, but swiping it also can time- and location-stamp me
 - Does the voting booth correctly record/transmit my vote?
- Of data destruction
 - Impossible to ensure?

Incentives

- Economic mechanisms?
 - Should people have graduated, not Boolean (opt-in/out) settings?
 - Privacy is not a fungible good
 - My privacy is more important to me than to you, and vice-versa
 - Economic mechanisms like negotiation change SW architectures
- What are the costs of privacy
 - Dollar costs?
 - E.g. black market value of identity today (assertion: \$60 per capita). Value chain that follows?
 - Frictional costs to doing business
 - Usability
 - E.g. people who work in unsafe human rights environments, where encryption can mean life or death, often do not have the time or means to employ it
 - E.g. P3P is rich but too difficult to understand, hence most users are left with one of k defaults for small k

Technology

- Authorization and Accountability.
 - Authorization scales poorly. Trust and punish (i.e. Accountability) scales more easily.
 - Debate: The above argument depends on the cost of an undetected violation.
- Graceful degradation.
 - Single point of control means that once something breaks it breaks big.
 - Does not matter once leaked it stays leaked.
- Failure mode: not all failures are equally bad
 - E.g. a database that erases itself when something happens vs. one which dumps all state.

Differences across types of users

- Corporations have quite a few legal rights that individuals do not have.
- Auditing privileges and mechanisms typically applied by government to organizations.
- What about auditing privileges and mechanisms for individuals?
 - Making sure that information out in the world about you is accurate.
 - You have the right to see and demand rectification of credit reporting information.

Education

- Convincing a computer scientist is not sufficient. Need to be understood and communicated to people.
 - Two way process.
 - Usually we try to work on problems that matter to people.
 - In this arena, we have to make what we are working on matter to people.
- Fostering a culture that respects privacy.
 - Trivial examples (grocery incentive cards) trivialize the problem.
 - People may not value privacy because examples they have seen are trivial.
 - Carrots vs. Sticks
 - High profile cases of privacy leakage
 - “Hacking” for consciousness-raising. Example of MIT students who bought used disk drives, recovered sensitive data, and published about it. Example of building a personal data portal that joins lots of public data on the web. Positive consciousness-raising? Harmful to individuals? Unnecessarily alarmist?