Vision Paper:
Enabling Privacy for Paranoids

Sandford University

Paper Review
Dan Matheson
CS 681, Spring 2005
Presentation Outline

• Motivation for paper
• P4P: Paranoid Platform of Privacy Preferences, Retaining Control
• Current privacy technologies
• Final thoughts
Motivation for Paper

• Lack of trust in a corporation's intentions for protecting a customers private data.
  – Recent history of violations
  – Recent history of data theft, Choice Point & Bank of America

• Lack of confidence in recent proposals to clarify privacy policies for the customer.
  – Still rely on trusting the organization collecting the data.
Motivation & Problems

- W3C Platform for Privacy Preferences (P3P)
  - Trust that the organization clearly states policies.
    - Confusing legalese
    - Imprecise terms
  - Trust that the organization will adhere to policies.
  - Trust that the organization has means to implement policies.
- Complexity of defining policies
- New HTTP response header
Motivations and Problems

• Hippocratic databases
  – Onus is still in hands of organization.
  – Customer's trust rules might be different from organization's rules so Hippocratic database do not help.
  – New philosophy of collecting the minimum data versus the old philosophy collect as much as possible because it might be useful in the future.
Goals of the Solution

- “We contend that control can be retained if the individual can release information to an organization such that the released information is unusable for illegitimate tasks.”
- P4P frame seeks to enable a person to control personal information after release to an organization.
Privacy Approaches

(a) Prevention

(b) Detection

(c) Containment
Retaining Control

- The primary mechanism is by placing an agent between an individual and an organization.
  - The individual has to only trust one entity.
  - The organization needs to trust many entities that might be untrustworthy.
Agent Capabilities

- **Timeout**
  - Limited time for use
- **Limited Use**
  - Maximum number of accesses
- **Restricted Source**
  - Agent will respond only to fixed sources
- **Invalidation**
  - Explicitly tell agent to stop
- **Isolation**
  - Release unique values to each different organization.
Retaining Control - Types

- Local identifiers
  - phone number, social security number

- Issues
  - Exiting applications that only accept certain forms
  - Dealing with duplicates
  - Privacy convenience trade-off

- Solution
  - Agent generates, perhaps from true identifier
  - Needs to be Unique, Opaque, Private, Independent
Retaining Control - Types

• Foreign-key identifiers
  • Used for interaction between multiple organizations

• Issues
  • Sharing an id for one organization with another for information exchange
  • Unsharing of identification values

• Solution
  • Share via agent, organizations must change operating processes
  • Needs to be Opt-in, Opaque, Opt-out
Retaining Control - Types

• Value predicates
  • The need to use a personal value, like age

• Issues
  • Hiding personal value
  • Easy to invert predicates
  • Giving false personal value to cheat

• Solution
  • Agent evaluates organization predicate
  • Notary agent or trusted third party
  • Needs to be Opaque, Verifiable
Retaining Control - Types

• Multi-source value predicates
  • The need to use multiple personal values

• Issues
  • Hide personal values, larger Quasi-identifier
  • Easy to invert predicate
  • Giving false values to cheat

• Solution
  • Trusted third party
  • Needs to be Opaque, Verifiable
P4P Solution

- Private information can be classified along 3 dimensions
  - Ownership
    - individual or organization
  - Type
    - Identifier, service handle, input to predicate, copy
  - Desired level of control
    - Complete privacy, limited time/use, no predicate input, no integration, accountability, sharable
P4P Solution

• An additional 3 areas need to be defined
  – Trust
    • Does trust match preferred information handling
  – Adversary Type
    • Passive, active, open-world
  – Interaction Properties
    • Traceability, revocability, isolation, minimality
Current Privacy Technologies

- Secure databases
- Trust management systems
- Statistical databases
- Anonymous networks
- Cryptography
- Hippocratic databases
Summary

• The other privacy papers took the position on the things that can be done from a developer / application standpoint to ensure privacy.

• This paper takes the view from and individual's standpoint. How can an individual limit their personal information distribution.

• Both approaches are needed.
Conclusions & Open Issues

• It will be problematic to cause some of the changes indicated in the industry relating to predicate value situations.

• While the agent approach looks promising, finding an agent that both sides trust will be difficult.

• The privacy policy expression mechanism is still far short of easy to formulate, understandable and broadly applicable (still need lawyers).
Conclusions & Open Issues

- The paper does not discuss another reason for agents: ensuring the currency and accuracy of the personal data.
- If the individual decides to give out personal data, how do they ensure the continuing integrity of that data? Perhaps by a digital signature on the data?
- How are the conflicts between data integrity balanced with anonymity requirements for data re-use within the privacy policy?
- Can agent use patterns provide a covert channel for defeating the anonymity that an agent provides?