Accountable Systems: Or, what does Law have to do with Computer Science?

Daniel J. Weitzner
Director, CSAIL Decentralized Information Group
Massachusetts Institute of Technology

March 3, 2014
Roadmap

• A short history of Computer Science and privacy
• Accountable Systems*: New strategies for meeting privacy challenges
• Various approaches to accountability
• Conclusion – what the world an look like with accountable systems and the right rules

*Full disclosure: Weitzner is co-founder of a startup venture developing policy analytics tools for enterprise systems.
Original computer science approach to privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Alan Westin, Privacy and Freedom (1967)
Jerry Salzer/Mike Schroeder (CACM 1974)
Unanswered Privacy Challenges

- Mine individual clinical data without risk of insurance discrimination
- Deliver personalized genomic medicine without employer misuse (GINA)
- Mine threat data without misuse of personal information
- Audited sharing with governments
- Mine metadata without harming innocent citizens (FISA)
- Locate terrorist signatures in big data without harm to citizens
- Target ad and prices fairly without misuse for credit purposes (FCRA/DAA)
- Assure consumers no misuse in hiring or insurance decisions

Health care delivery and research

Law Enforcement and national security

Cyber-security

Marketing Profiles
Trust Challenge

Judge Reggie B. Walton, Chief Judge, Foreign Intelligence Surveillance Court

“the court lacks the tools to independently verify how often the government’s surveillance breaks the court’s rules that aim to protect Americans’ privacy”

- Washington Post, August 15, 2013
Information Accountability

When information has been used, it should be possible to determine what happened, and to pinpoint use that is inappropriate.

Policy analytics yields human-readable result with explanation.

Explanation: “illegal to use health information as a condition of delivering a public service”

“Service denial violates anti-discrimination law”
Mass. Gen. Law Chapter 6: Section 172. Dissemination of record information; certification; eligibility for access; scope of inquiry; listing; access limited; rules; use of information

Section 172. Except as otherwise provided in this section and sections one hundred and seventy-three to one hundred and seventy-five, inclusive, criminal offender record information, and where present, evaluative information, shall be disseminated, whether directly or through any intermediary, only to (a) criminal justice agencies; (b) such other agencies and individuals required to have access to such information by statute including United States Armed Forces recruiting offices for the purpose of determining whether a person enlisting has been convicted of a felony as set forth in Title 10, section 504 of the United States Code; to the active or organized militia of the commonwealth for the purpose of determining whether a person enlisting has been convicted of a felony, and (c) any other agencies and individuals where it has been determined that the public interest in disseminating such information to these parties clearly outweighs the interest in security and privacy. The extent of such access shall be limited to that necessary for the actual performance of the criminal justice duties of criminal justice agencies under clause (a); to that necessary for the actual performance of the statutory duties of agencies and individuals granted access under clause (b); and to that necessary for the actual performance of the actions or duties sustaining the public interest as to agencies or individuals granted access under clause (c). Agencies or individuals granted access under clause (c) shall be eligible to receive criminal offender record information obtained through interstate systems if the board determines that such information is necessary for the performance of the actions or duties sustaining the public interest with respect to such agencies or individuals.

The board shall certify those agencies and individuals requesting access to criminal offender record information that qualify for such access under clauses (a) or (b) of this section, and shall specify for each such agency or individual certified, the extent of its access. The board shall make a finding in writing of eligibility, or noneligibility of each such agency or individual which requests such access. No such information shall be disseminated to any agency or individual prior to the board’s determination of eligibility, or, in cases in which the board’s decision is appealed, prior to the final judgment of a court of competent jurisdiction that such agency or individual is so eligible.

No agency or individual shall have access to criminal offender record information under clause (c), unless the board, by a two-thirds majority of the members present and voting, determines and certifies that the public interest in disseminating such information to such party clearly outweighs the interest in security and privacy. The extent of access to such information under clause (c) shall also be determined by such a two-thirds majority vote of the board. Certification for access under clause (c) may be either access to information relating to a specific identifiable individual, or individuals, on a single occasion; or a general grant of access for a specified period of time not to exceed two years. A general grant of access need not relate to a request for access by the party or parties to be certified. Except as otherwise provided in this paragraph the procedure and requirements for certifying agencies and individuals under clause (c) shall be according to the provisions of the preceding paragraphs of this section.

Each agency holding or receiving criminal offender record information shall maintain, for such period as the board shall determine, a listing of the agencies or individuals to which it has released or communicated such information. Such listings, or reasonable samples thereof, may from time to time, be reviewed by the board or the council to determine whether any statutory provisions or regulations have been violated. …
Each policy is represented as:
- rules and patterns in a policy file
- definitions and classifications in an ontology file.
Simple Compliance Answer

"Transaction is compliant with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172."
[Recipient,] Fred Agenti, is a member of a Criminal Justice Agency…

Inquiry is about Robert B. Guy and is based on a personally identifying characteristic…

Inquiry is about Robert B. Guy and is based on a personally identifying characteristic, as required by MGL 6-172 Para. 5, Sent. 1, Cl. 2.

“[Recipient,] Fred Agenti, is a member of a Criminal Justice Agency…”

“Inquiry is about Robert B. Guy and is based on a personally identifying characteristic…”
Accountable Systems Architecture

- Expressivity
- Evaluation of usage post-collection & analysis
- Explanation
- Support incompleteness and inconsistency
Accountable Systems Research – Formalizing system behavior to conform to policy

- Policy languages and reasoners: compliance check and explanation [KBKJBH2010]
- Inferring purposes and other properties through statistical methods [TschantzDattaWing2013]
- Formal definition of accountable systems to assess reliability of systems [FeigenbaumJaggardWright2011]
- Operating System and Hardware-level architectures to ground enforcement and accountability in silicon [YXZK2009]
A Goal by Analogy: Financial Accounting

General Ledger Transactions

Financial Balance Sheet

- Assets
  - ...
  - Liabilities
  - ...
  - Net Assets
  - Owners Equity

Accounting rules

Public Trust
Personal Information Accountability

Personal Information Transactions

Personal Information Balance Sheet

Compliance
- FCRA#
- DAA#
- FISA#
- ECPA#

Non-compliance
- FCRA#
- DAA#
- FISA#
- ECPA#

Total Transactions

Net Accountability

Public Trust

Accountable Systems Reasoning
The world with Accountable Systems

- Share health information for research without risk of insurance bias
- Share location with friends without fear of intrusive tracking
- Leverage the power of the Web for democracy without chilling political activity
- Participate in social networking without risk of job loss
- Allow behavior profiling without risking financial discrimination
References

- Weitzner, Needles in Haystacks: Creating Information Balance Sheets for Personal Data, Remarks before the United States Privacy and Civil Liberties Oversight Board Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of Foreign Intelligence Surveillance Act, July 9, 2013
- Senevirante, Augmenting the Web with Accountability, World Wide Web Conference 2012 PhD Symposium, April 2012
- For more: http://dig.csail.mit.edu/