Information Accountability

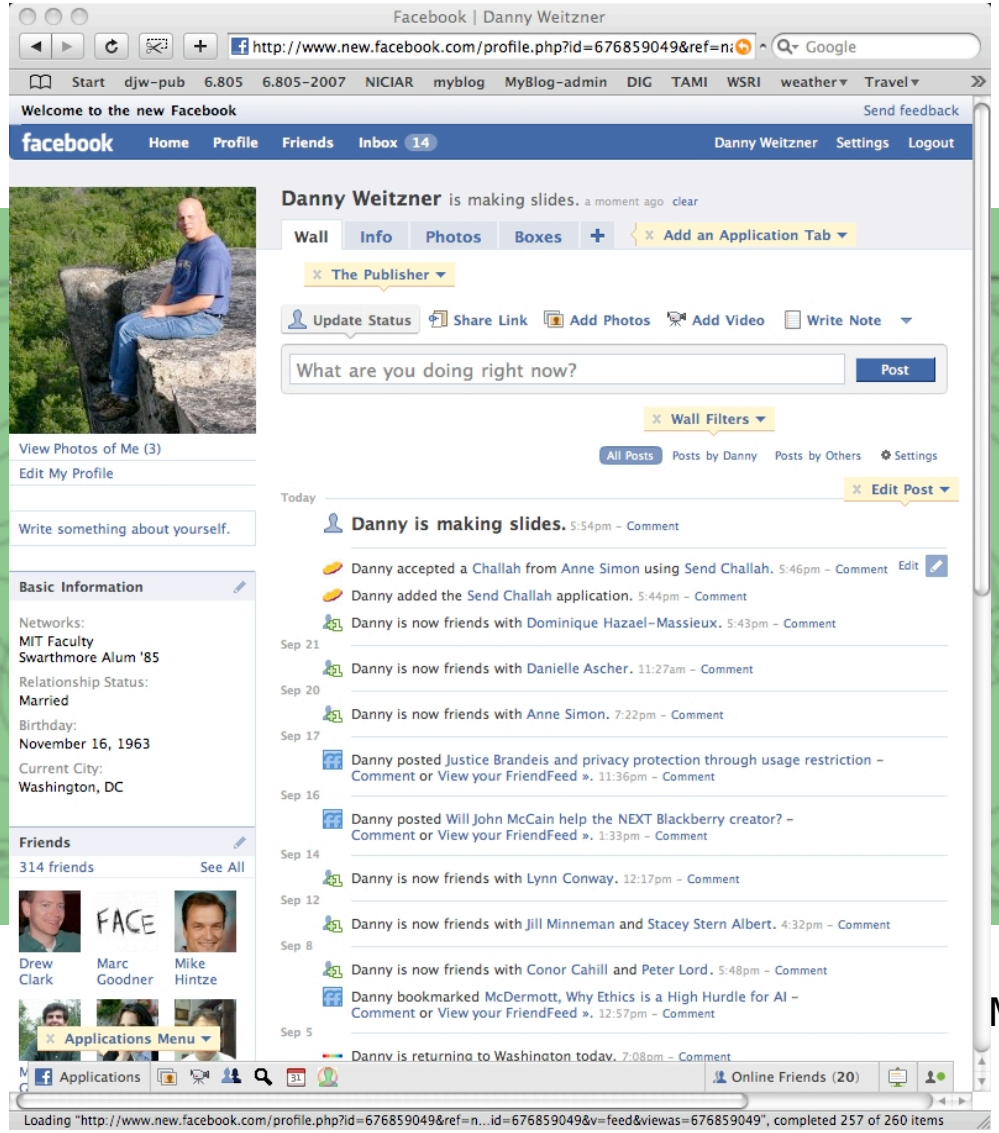
Re-thinking legal and technical approaches to privacy protection in the era of the Web

Center for Embedded Network Sensing
6th Annual Research Review
22 October 2008

Daniel J. Weitzner djweitzner@csail.mit.edu
MIT CSAIL Decentralized Information Group
http://dig.csail.mit.edu/

Getting over Scott McNealy

Motivation: Privacy in transparent environments



Mistree (2007)

How to get over ‘getting over’ privacy

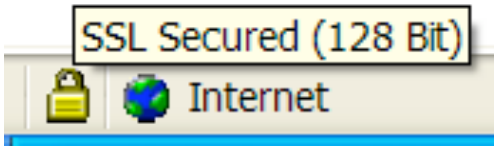
- Step 1 – Drop the fig leaf: admit just how broken our legal and technical privacy tools actually are.
- Step 2 – Learn the lessons of accountability from other areas of law and society.
- Step 3 – Build Accountable Systems.
- Step 4 – Find new projects for cryptographers.

Step 1

Drop the fig leaf: admit just how broken our legal and technical privacy tools actually are.

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)
Saltzer/Schroeder (CACM 1974)



Changing Views of Privacy?

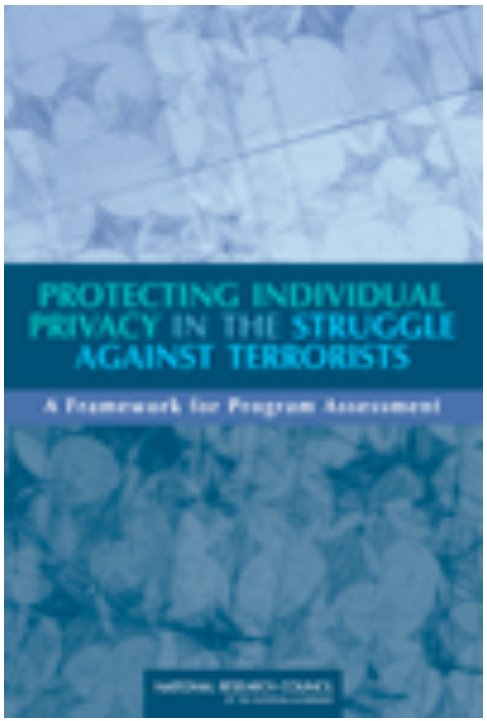
Shape of things to come

"GINA prevents health insurers from denying coverage, adjusting premiums on the basis of genetic information, or requesting that an individual undergo a genetic test. Similarly, employers are *prohibited from using* genetic information to make hiring, firing, or promotion decisions."

Genetic Information Non-Discrimination Act of 2008

National Academy of Sciences

- Conclusion 5. The *current policy regime does not adequately address violations of privacy that arise from information-based programs* using advanced analytical techniques, such as state-of-the-art data mining and record linkage.
- Recommendation 2. The U.S. government should periodically review the nation's laws…. Such reviews should consider *establishment of restrictions on how personal information can be used*. Currently, legal restrictions are focused primarily on how records are collected and assessed, rather than on their use.



Protecting individual Privacy in the Struggle Against Terrorists
National Academy of Sciences, 2008.

New Approaches to Privacy Policy

"As president, Barack Obama will strengthen privacy protections for the digital age and will harness the power of technology to hold government and business accountable for violations of personal privacy….Barack Obama *supports restrictions on how information may be used and technology safeguards to verify how the information has actually been used*."

TECHNOLOGY AND INNOVATION FOR A NEW GENERATION.
Sen. Barak Obama,
Feb. 2007

New definition of 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*~~ *used by* others.

Information Accountability

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

Weitzner et al. (CACM June 2008)

Step 2

Learn the lessons of accountability from other areas of law and society.

Quiz

1. How many believe you are subject to law (any law)?
2. How many of you follow (most) laws? [exclude speed limits]
3. How many of you read all the laws to which you believe you are subject?
4. How many have been to a court of law?

Key finding: most of us follow rules even when we are able to violate them.

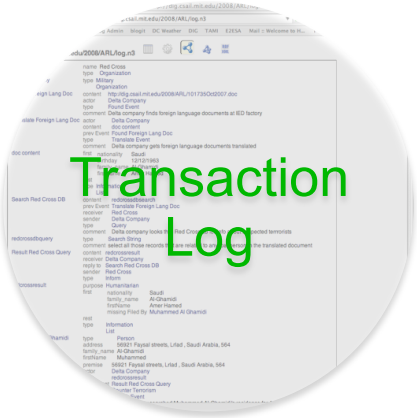
Regulatory Patterns for Large Scale Information Flows

- **Fair Credit Reporting Act**
  - Nearly unlimited information collection
  - Unlimited analysis
  - Strict **usage** limits
  - Harsh penalties for mis-use
  - Feedback loop to ensure accuracy
- **Securities Laws**
  - required reports
  - significant penalities for failure to file
  - virtually no review of substance of reports unless some stops trouble
  - criminal penalty for misreporting

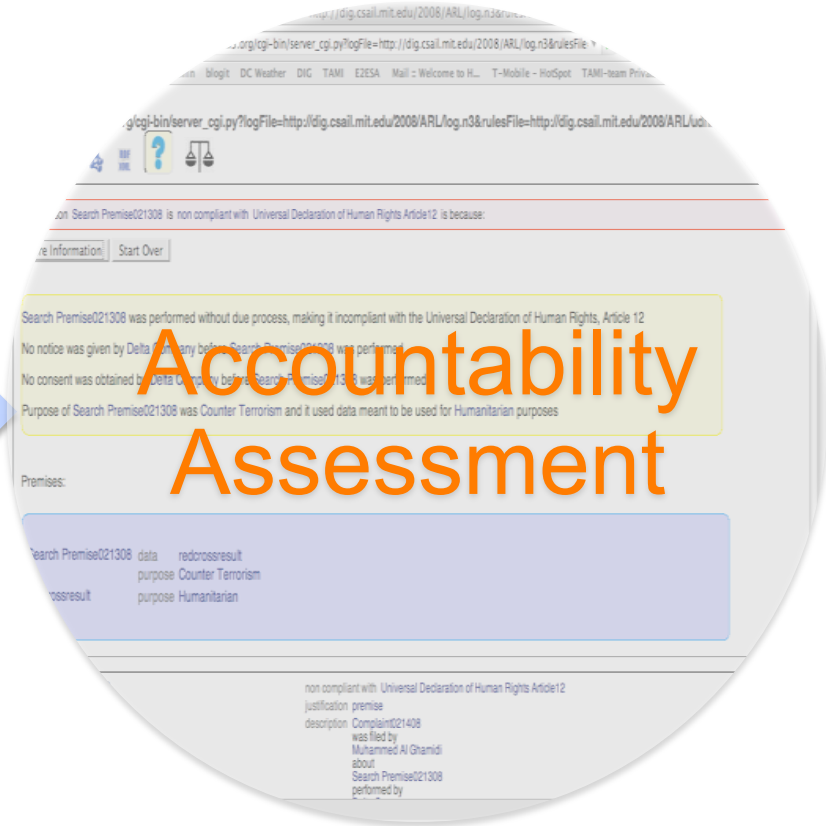
Step 3

Build accountable systems.

Accountable Systems

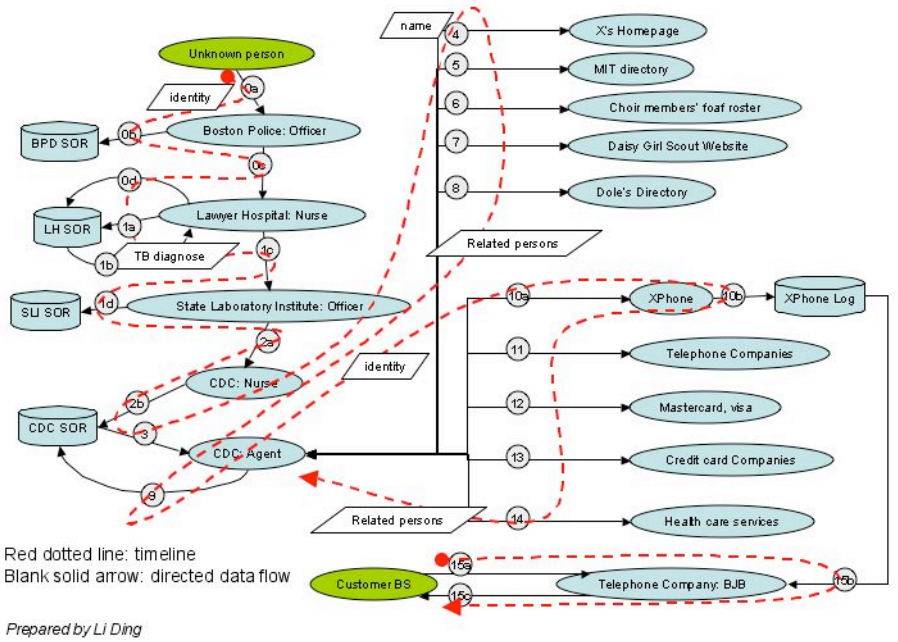


AIR
Reasoner

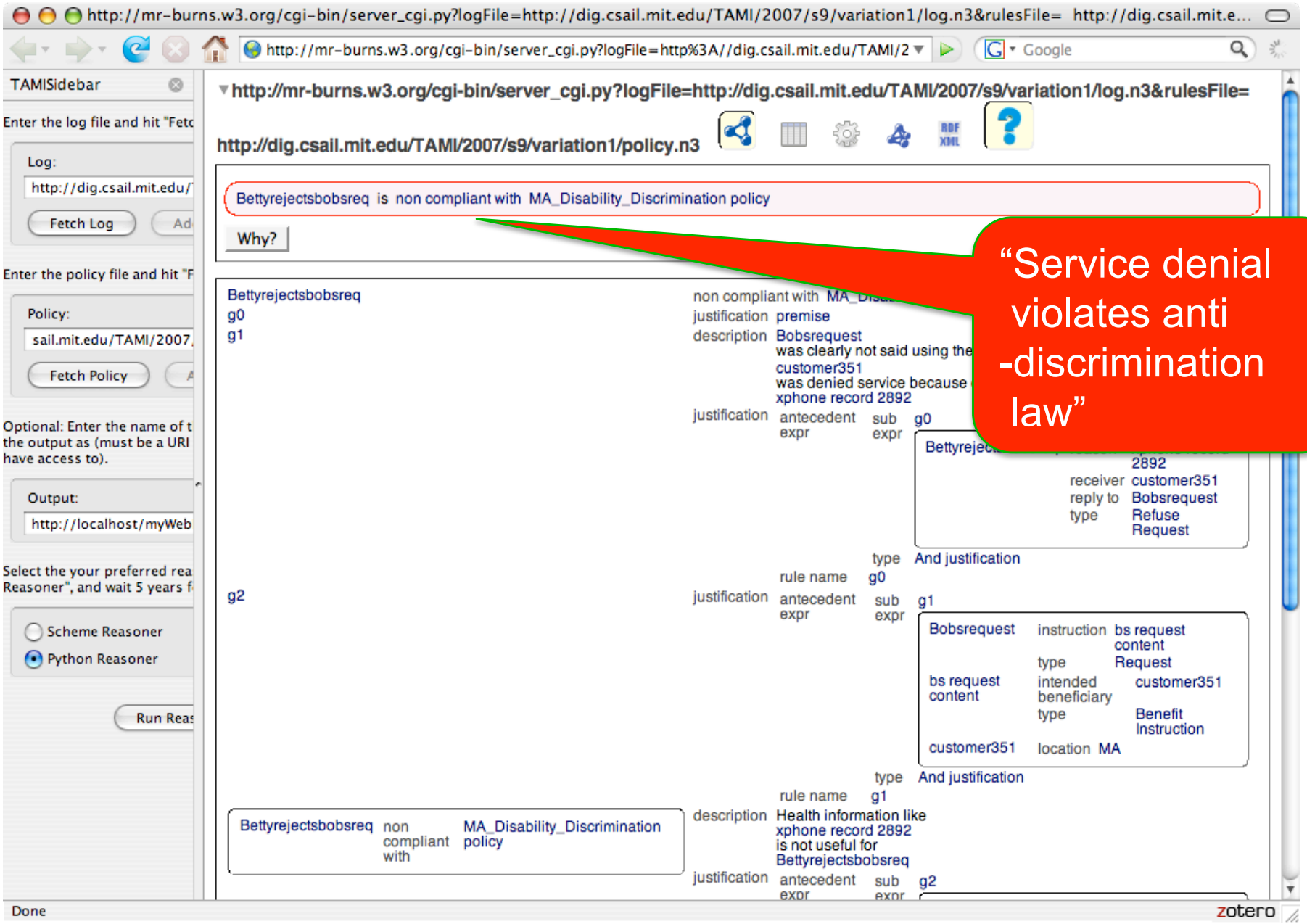


Scenario

- In order to prevent an epidemic, CDC contacts everyone whom an unconscious tuberculosis patient could have been in contact with
  - people he works with, his choir, the members of his scout troop, people h has called, who have called him
- CDC gets his phone records from Xphone
- Sometime later Bob Same has phone troubles and calls XPhone to schedule an appt
- The customer service operator sees that CDC had obtained his records and infers that he must have some contagious disease
- So she refuses to schedule a repairman



Human-readable result



Human-readable result with explanation

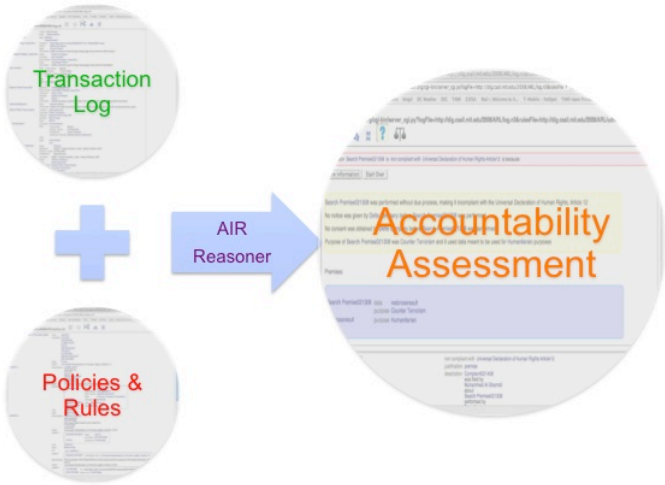
Copyright license compliance

http://mr-burns.w3.org/cgi-bin/server_cgi.py?logFile=http://dig.csail.mit.edu/TAMI/2008/CreativeCommons/AIR_Rules/BY_log_non_compliant.n3&rulesFile=http://dig.csail.mit.edu/TAMI/2008/CreativeCommons/AIR_Rules/BY_Policy.n3

"Use of photo violates license because no attribution found"

Dependency Tracking

- AIR: rule-based policy language for usage rules and access control
- integrated explanations for policy decisions through dependency tracking
- Truth Maintenance System (TMS)
  - track of the logical structure of a derivation
  - ability to assume and retract hypothetical premises
  - more efficient and expressive reasoning through the use of goal direction
- grounded in Semantic Web technologies for greater interoperability, reusability, and extensibility

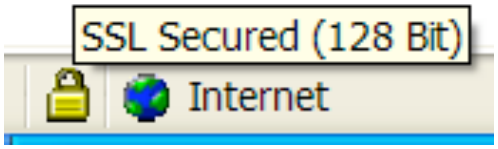


Step 4

Find new jobs for computer security researchers (besides privacy protection). ☺

Limits of cryptographic security for privacy protection

- Rules must be susceptible enforcement by a priori action
- Application of rules to ground facts must be automatically decidable without human intervention



Anti-formalism: lessons from the software verification debate

"[T]he proof of a theorem is a message", not a an formal abstraction that ties it completely and irrefutably to ground truths.

De Millo, Lipton, Perlis, "Social Processes and Proofs of Theorems and Programs." CACM, May 1979 (Vol. 22 No. 5), p. 271

- **Proofs gain support by**
  - Readability
  - Peer review
  - Effectiveness in the mathematical world
- **But software verifications**
  - Can't be read
  - Are inherently complex beyond human explanation

Source of confidence in anti-formalist world view

Common Mistake

- Seeking perfect *a priori* enforcement of legal/social rules
- Attempting to design formally verifiable system

Accountable Systems

- Seek simplicity over perfection
- Provide human-accessible explanation
- Create communicable basis for community acceptance

Coda: Harvard Personal Genetics Project

"Developments in both medical informatics and bioinformatics show that the guarantee of *absolute privacy and confidentiality is not a promise that medical an scientific researchers can deliver* any longer."

"[B]uilding of any comprehensive genotype–phenotype data collection requires that the individuals be fully aware that the data can be and likely will be accessed, shared and linked to other sets of information, and that the full purpose and the extent of further usage cannot be foreseen.

"From genetic privacy to open consent," Nature Review Genetics 9, 406-411 (May 2008)

More Information

- Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, Sussman, Information Accountability, *Communications of the ACM, Jun. 2008, 82-87.*
- C. Hanson, L. Kagal, D. Weitzner, **"Integrated Policy Explanations via Dependency Tracking"** (To appear IEEE Policy 2008)
- D. Weitzner, "Beyond Secrecy: New Privacy Protection Strategies for Open Information Spaces," IEEE Internet Computing, Sept/Oct 2007. http://dig.csail.mit.edu/2007/09/ieee-ic-beyond-secrecy-weitzner.html
- Feigenbaum and Weitzner (eds.), "Report on the 2006 TAMI/Portia Workshop on Privacy and Accountability." http://dig.csail.mit.edu/2006/tami-portia-accountability-ws/summary
- **Air specifications: http://dig.csail.mit.edu/TAMI/2007/AIR/**
- **Demos and code:** http://dig.csail.mit.edu/TAMI/2008/JustificationUI/howto.html