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

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

CSAIL

Roadmap

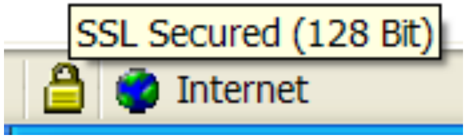
- A short history of Computer Science and privacy
- Accountable Systems*: New strategies for meeting privacy challenges
- Various approaches to accountability
- Conclusion – what the world an look like with accountable systems and the right rules

**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.

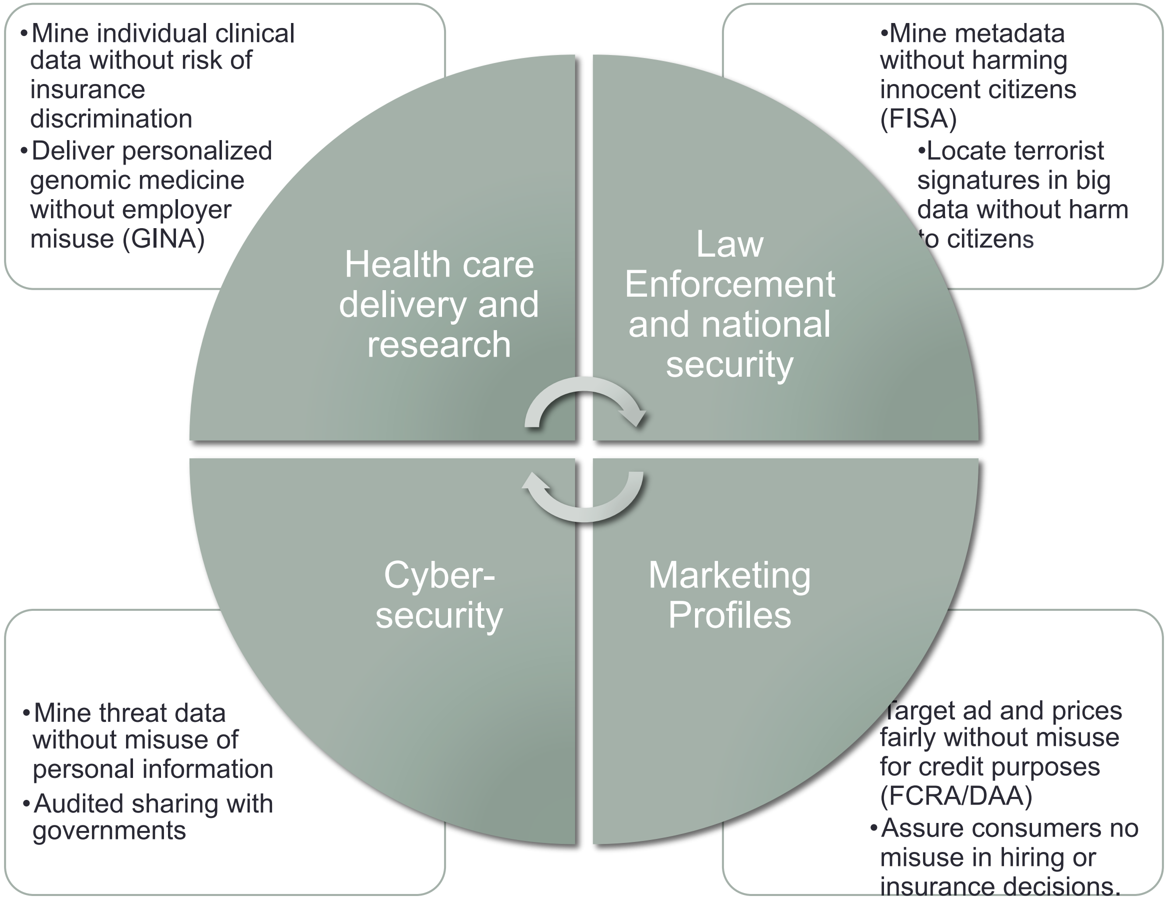
Alan Westin, Privacy and Freedom (1967)
Jerry Salzer/Mike Schroeder (CACM 1974)



SSL Secured (128 Bit)

Internet

Unanswered Privacy Challenges



Health care delivery and research

- Mine individual clinical data without risk of insurance discrimination
- Deliver personalized genomic medicine without employer misuse (GINA)

Law Enforcement and national security

- •Mine metadata without harming innocent citizens (FISA)
  - •Locate terrorist signatures in big data without harm to citizens

Cyber-security

- Mine threat data without misuse of personal information
- Audited sharing with governments

Marketing Profiles

- Target ad and prices fairly without misuse for credit purposes (FCRA/DAA)
- Assure consumers no misuse in hiring or insurance decisions.

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"

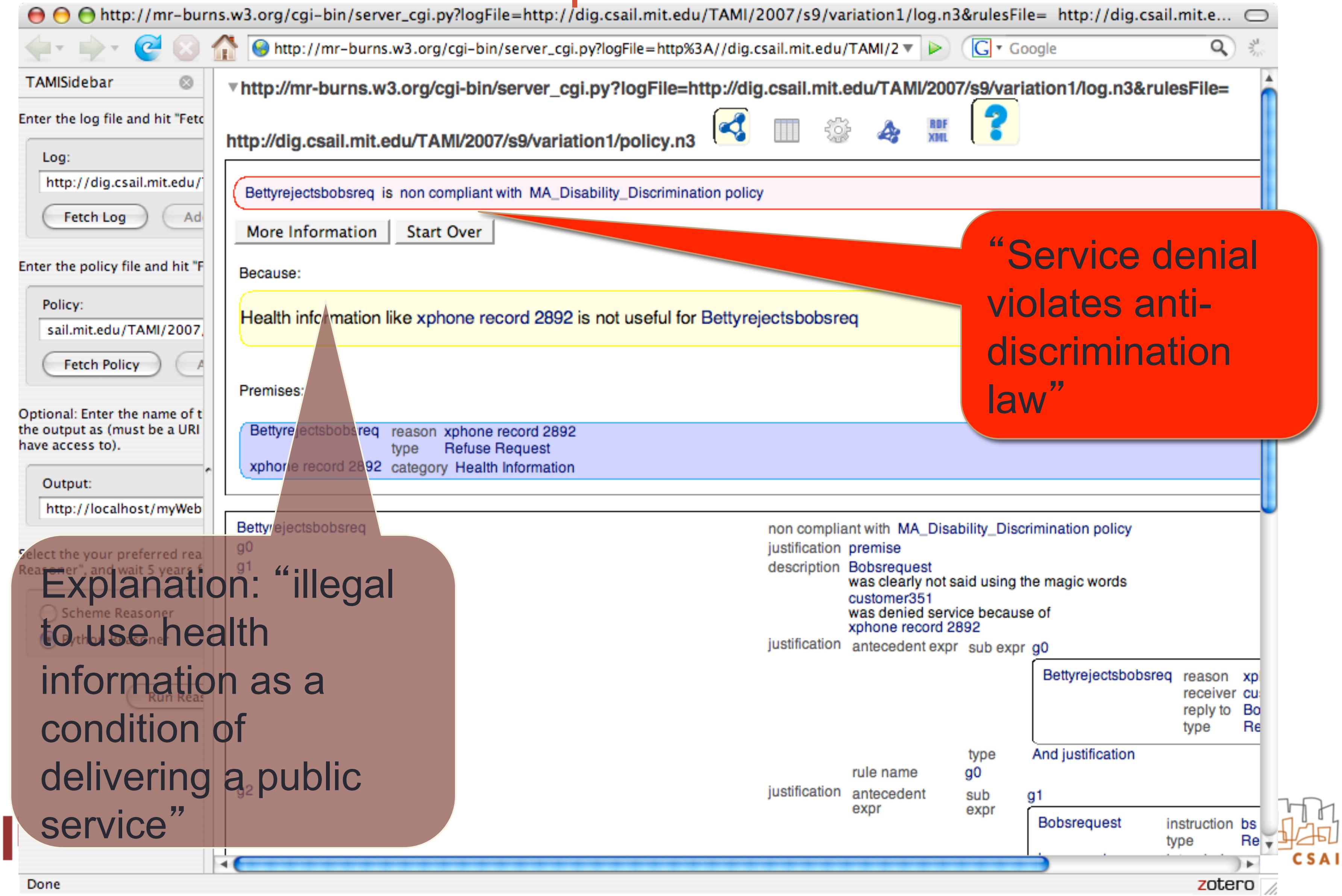
- Washington Post, August 15, 2013

Information Accountability

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

“Information Accountability,” Weitzner, D. J., Abelson, H., Berners-Lee, T., *et al.*
Communications of the ACM (Jun. 2008), 82-87.

Policy analytics yields human-readable result with explanation



http://mr-burns.w3.org/cgi-bin/server_cgi.py?logFile=http://dig.csail.mit.edu/TAMI/2007/s9/variation1/log.n3&rulesFile= http://dig.csail.mit.e...

http://mr-burns.w3.org/cgi-bin/server_cgi.py?logFile=http%3A//dig.csail.mit.edu/TAMI/2

TAMISidebar

Enter the log file and hit "Fetc

Log: http://dig.csail.mit.edu/

Fetch Log

Enter the policy file and hit "F

Policy: sail.mit.edu/TAMI/2007,

Fetch Policy

Optional: Enter the name of t the output as (must be a URI have access to).

Output: http://localhost/myWeb

Select the your preferred rea Reasoner", and wait 5 years f

○ Scheme Reasoner

● Python Reasoner

Run Reas

http://mr-burns.w3.org/cgi-bin/server_cgi.py?logFile=http://dig.csail.mit.edu/TAMI/2007/s9/variation1/log.n3&rulesFile= http://dig.csail.mit.edu/TAMI/2007/s9/variation1/policy.n3

Bettyrejectsbobsreq is non compliant with MA_Disability_Discrimination policy

More Information | Start Over

Because:

Health information like xphone record 2892 is not useful for Bettyrejectsbobsreq

Premises:

Bettyrejectsbobsreq	reason	xphone record 2892
	type	Refuse Request
xphone record 2892	category	Health Information

Bettyrejectsbobsreq
g0
g1
g2

non compliant with MA_Disability_Discrimination policy
justification premise
description Bobsrequest was clearly not said using the magic words customer351 was denied service because of xphone record 2892
justification antecedent expr sub expr g0

Bettyrejectsbobsreq	reason	xp
	receiver	cu
	reply to	Bo
	type	Re

type And justification
rule name g0
justification antecedent expr sub expr g1

Bobsrequest	instruction	bs
	type	Re

Done

"Service denial violates anti-discrimination law"

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

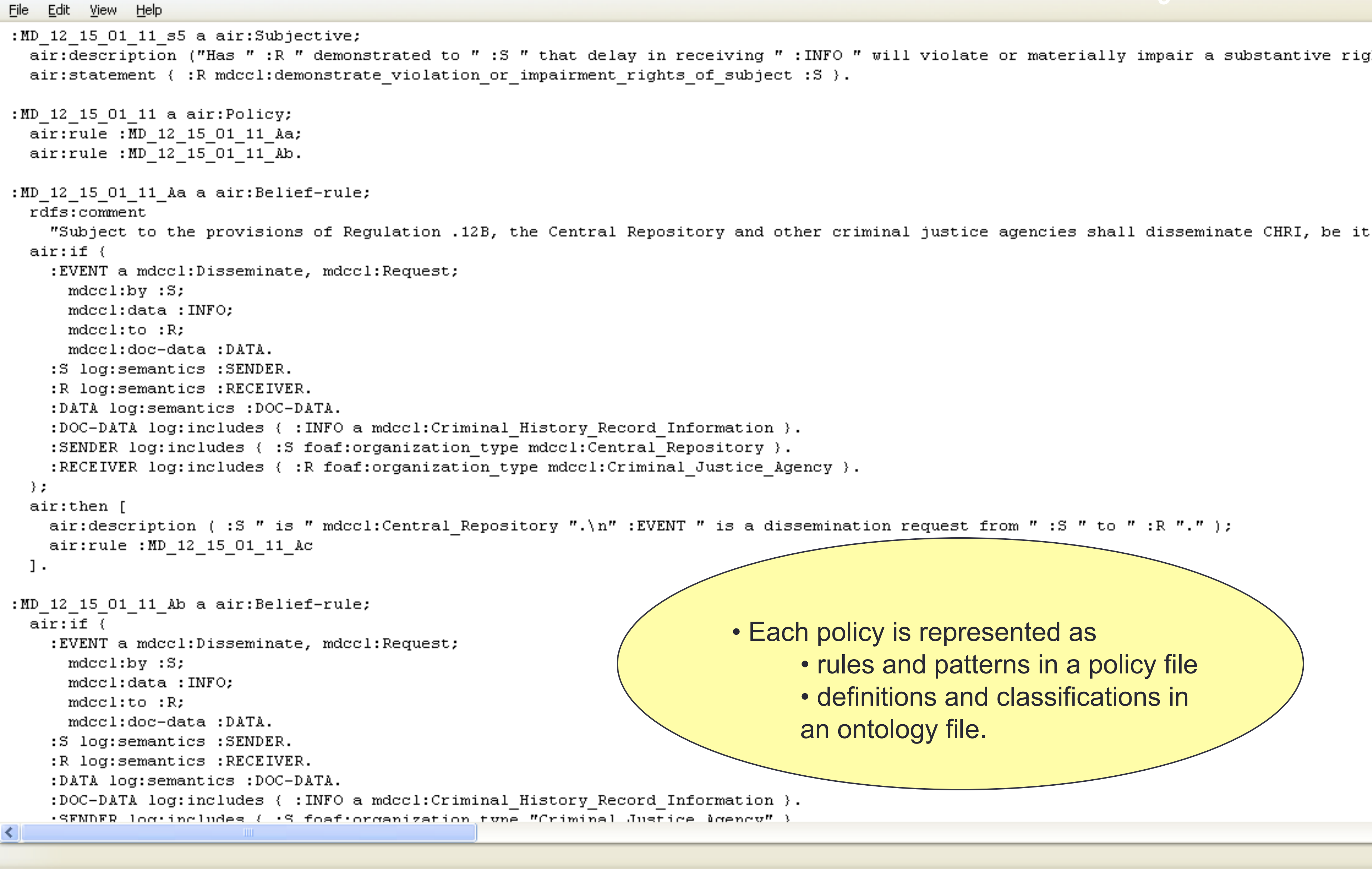
Mass. Gen. Law Chapter 6: Section 172. Dissemination of record information; certification; eligibility for access; scope of inquiry; listing; access limited; rules; use of information

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.

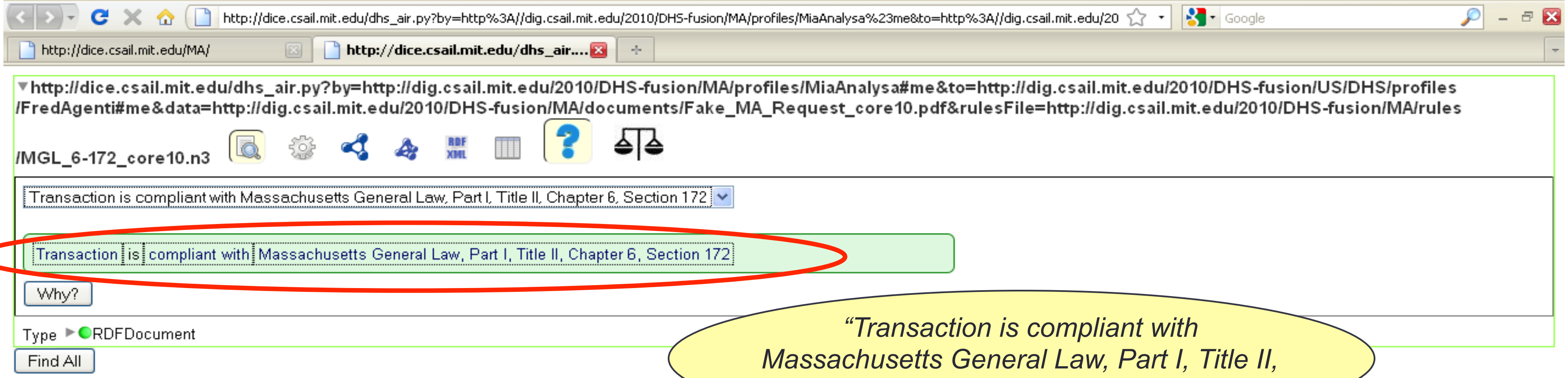
Each agency holding or receiving criminal offender record information shall maintain, for such period as the board shall determine, a listing of the agencies or individuals to which it has released or communicated such information. Such listings, or reasonable samples thereof, may from time to time, be reviewed by the board or the council to determine whether any statutory provisions or regulations have been violated. …



```
:MD_12_15_01_11_s5 a air:Subjective;
  air:description ("Has " :R " demonstrated to " :S " that delay in receiving " :INFO " will violate or materially impair a substantive rig
  air:statement { :R mdccl:demonstrate_violation_or_impairment_rights_of_subject :S }.

:MD_12_15_01_11 a air:Policy;
  air:rule :MD_12_15_01_11_Aa;
  air:rule :MD_12_15_01_11_Ab.

:MD_12_15_01_11_Aa a air:Belief-rule;
  rdfs:comment
    "Subject to the provisions of Regulation .12B, the Central Repository and other criminal justice agencies shall disseminate CHRI, be it
  air:if {
    :EVENT a mdccl:Disseminate, mdccl:Request;
      mdccl:by :S;
      mdccl:data :INFO;
      mdccl:to :R;
      mdccl:doc-data :DATA.
    :S log:semantics :SENDER.
    :R log:semantics :RECEIVER.
    :DATA log:semantics :DOC-DATA.
    :DOC-DATA log:includes { :INFO a mdccl:Criminal_History_Record_Information }.
    :SENDER log:includes { :S foaf:organization_type mdccl:Central_Repository }.
    :RECEIVER log:includes { :R foaf:organization_type mdccl:Criminal_Justice_Agency }.
  };
  air:then [
    air:description ( :S " is " mdccl:Central_Repository ".\n" :EVENT " is a dissemination request from " :S " to " :R "." );
    air:rule :MD_12_15_01_11_Ac
  ].

:MD_12_15_01_11_Ab a air:Belief-rule;
  air:if {
    :EVENT a mdccl:Disseminate, mdccl:Request;
      mdccl:by :S;
      mdccl:data :INFO;
      mdccl:to :R;
      mdccl:doc-data :DATA.
    :S log:semantics :SENDER.
    :R log:semantics :RECEIVER.
    :DATA log:semantics :DOC-DATA.
    :DOC-DATA log:includes { :INFO a mdccl:Criminal_History_Record_Information }.
    :SENDER log:includes { :S foaf:organization_type "Criminal_Justice_Agency" }.
```

- Each policy is represented as
  - rules and patterns in a policy file
  - definitions and classifications in an ontology file.

Simple Compliance Answer



http://dice.csail.mit.edu/dhs_air.py?by=http%3A//dig.csail.mit.edu/2010/DHS-fusion/MA/profiles/MiaAnalysa%23me&to=http%3A//dig.csail.mit.edu/20

Google
http://dice.csail.mit.edu/MA/
http://dice.csail.mit.edu/dhs_air....

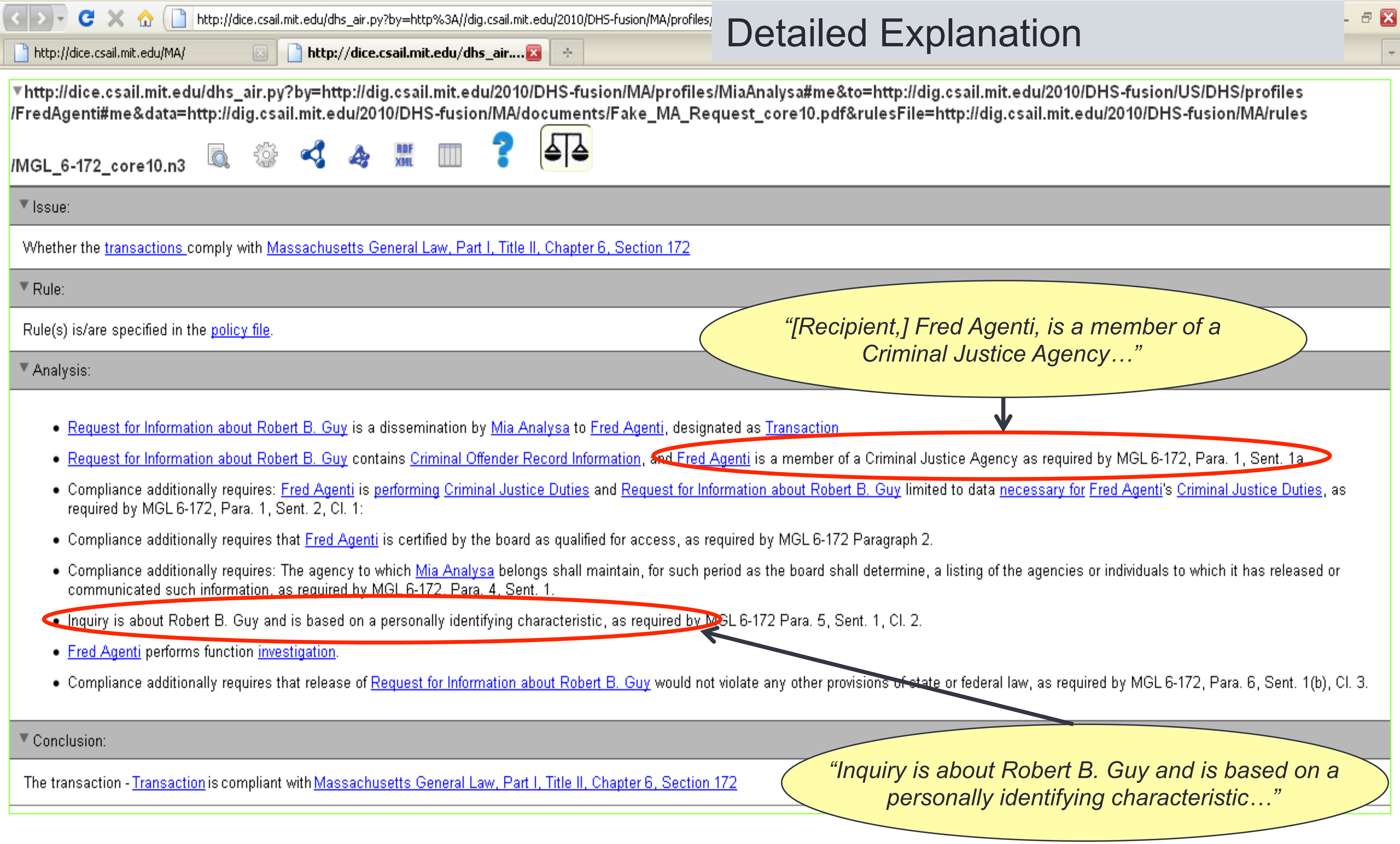
▼http://dice.csail.mit.edu/dhs_air.py?by=http://dig.csail.mit.edu/2010/DHS-fusion/MA/profiles/MiaAnalysa#me&to=http://dig.csail.mit.edu/2010/DHS-fusion/US/DHS/profiles/FredAgenti#me&data=http://dig.csail.mit.edu/2010/DHS-fusion/MA/documents/Fake_MA_Request_core10.pdf&rulesFile=http://dig.csail.mit.edu/2010/DHS-fusion/MA/rules/MGL_6-172_core10.n3

Transaction is compliant with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172

Transaction is compliant with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172

"Transaction is compliant with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172."

Detailed Explanation



http://dice.csail.mit.edu/dhs_air.py?by=http%3A//dig.csail.mit.edu/2010/DHS-fusion/MA/profiles/
http://dice.csail.mit.edu/MA/
http://dice.csail.mit.edu/dhs_air....
RDF XML
?

▼http://dice.csail.mit.edu/dhs_air.py?by=http://dig.csail.mit.edu/2010/DHS-fusion/MA/profiles/MiaAnalysa#me&to=http://dig.csail.mit.edu/2010/DHS-fusion/US/DHS/profiles/FredAgenti#me&data=http://dig.csail.mit.edu/2010/DHS-fusion/MA/documents/Fake_MA_Request_core10.pdf&rulesFile=http://dig.csail.mit.edu/2010/DHS-fusion/MA/rules/MGL_6-172_core10.n3

▼ Issue:

Whether the transactions comply with Massachusetts General Law, Part I, Title II, Chapter 6, Section 172

▼ Rule:

Rule(s) is/are specified in the policy file.

▼ Analysis:

- Request for Information about Robert B. Guy is a dissemination by Mia Analysa to Fred Agenti, designated as Transaction
- Request for Information about Robert B. Guy contains Criminal Offender Record Information, and Fred Agenti is a member of a Criminal Justice Agency as required by MGL 6-172, Para. 1, Sent. 1a
- Compliance additionally requires: Fred Agenti is performing Criminal Justice Duties and Request for Information about Robert B. Guy limited to data necessary for Fred Agenti's Criminal Justice Duties, as required by MGL 6-172, Para. 1, Sent. 2, Cl. 1:
- Compliance additionally requires that Fred Agenti is certified by the board as qualified for access, as required by MGL 6-172 Paragraph 2.
- Compliance additionally requires: The agency to which Mia Analysa belongs 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, as required by MGL 6-172, Para. 4, Sent. 1.
- 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.
- Fred Agenti performs function investigation.
- Compliance additionally requires that release of Request for Information about Robert B. Guy would not violate any other provisions of state or federal law, as required by MGL 6-172, Para. 6, Sent. 1(b), Cl. 3.

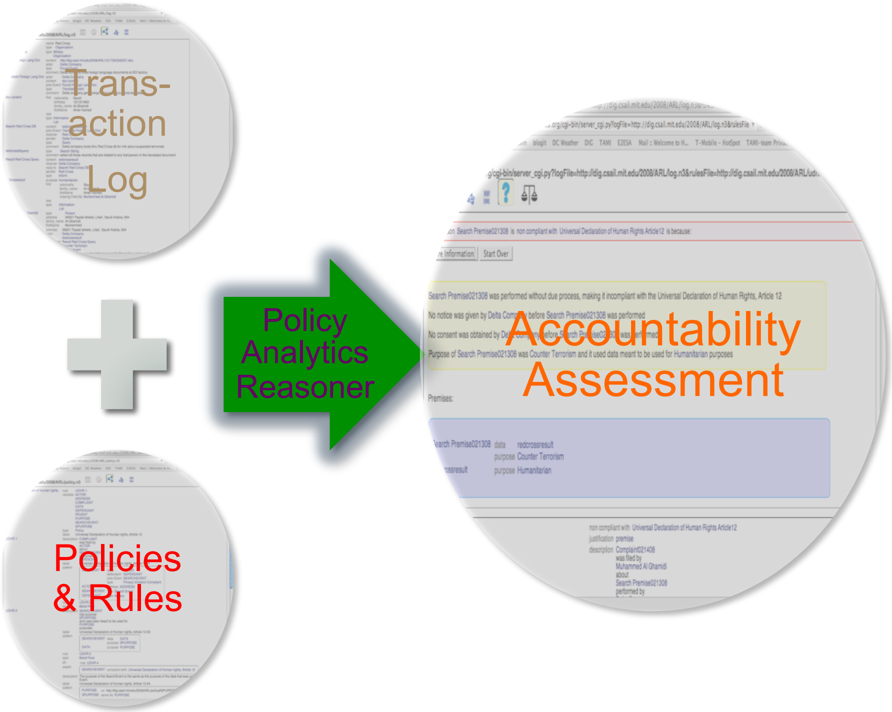
▼ Conclusion:

The transaction - 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…"

Accountable Systems Architecture



Search Premise021308 is non compliant with Universal Declaration of Human Rights Article12 is because:

Start Over

Search Premise021308 was performed without due process, making it incompliant with the Universal Declaration of Human Rights, Article 12

No notice was given by Delta Company before Search Premise021308 was performed

No consent was obtained by Delta Company before Search Premise021308 was performed

Purpose of Search Premise021308 was Counter Terrorism and it used data meant to be used for Humanitarian purposes

Premises:

Search Premise021308 data redcrossresult
purpose Counter Terrorism
redcrossresult purpose Humanitarian

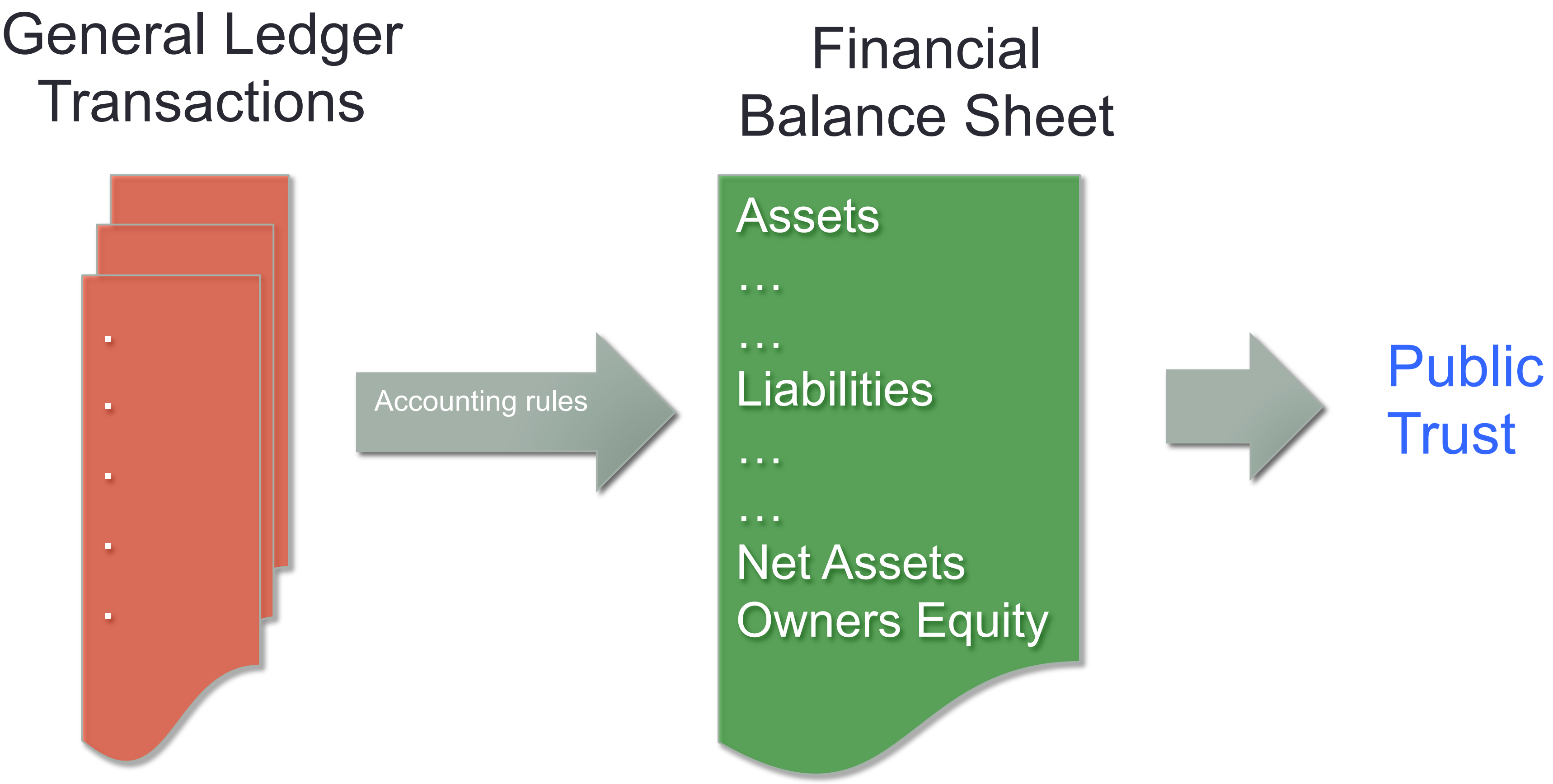
non compliant with Universal Declaration of Human Rights Article12
justification premise
description Complaint021408 was filed by Muhammed Al Ghamidi about Search Premise021308 performed by

- 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

Accounting rules

Financial Balance Sheet

Assets

…

…

Liabilities

…

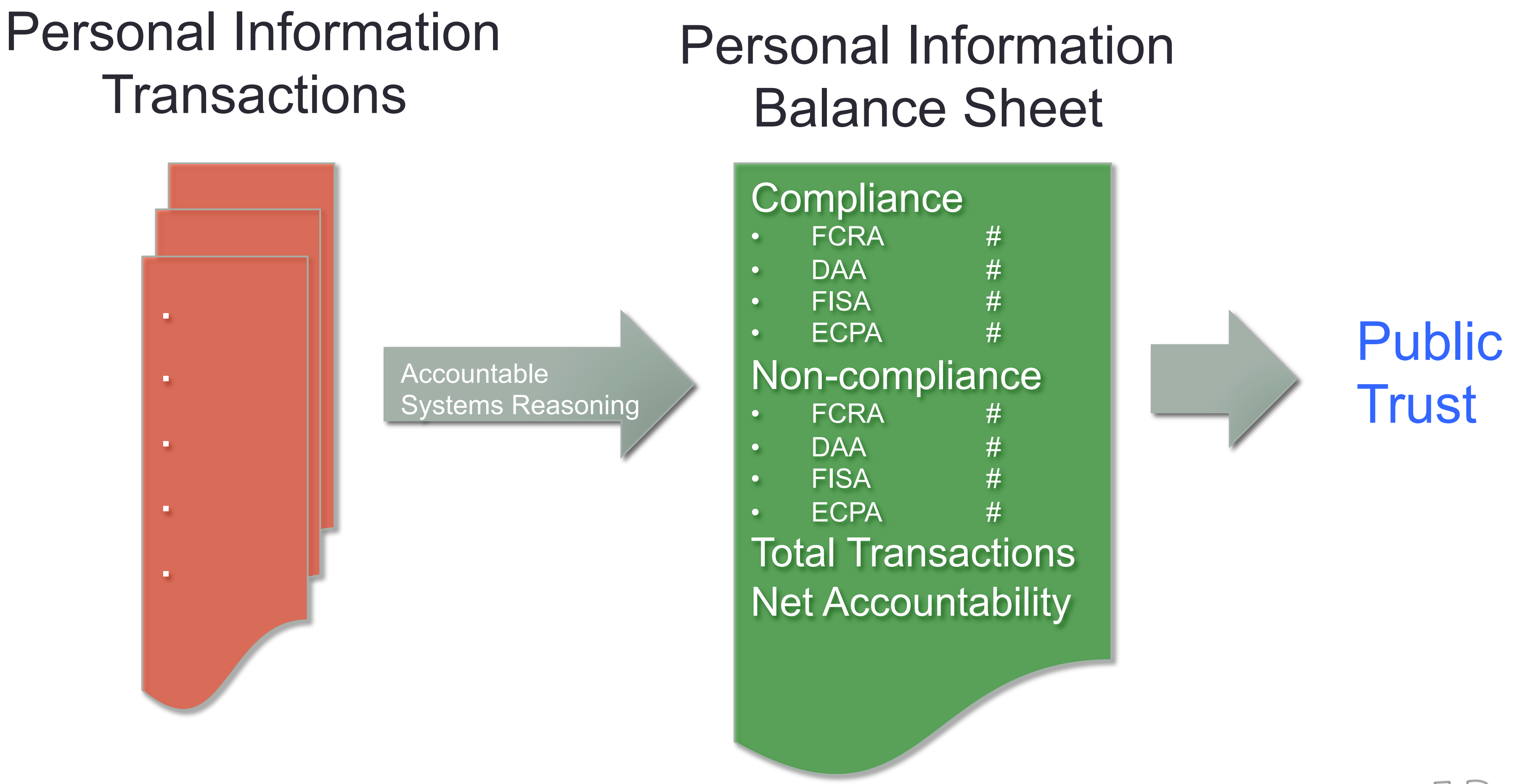
…

Net Assets

Owners Equity

Public Trust

Personal Information Accountability



Personal Information Transactions

Accountable Systems Reasoning

Personal Information Balance Sheet

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

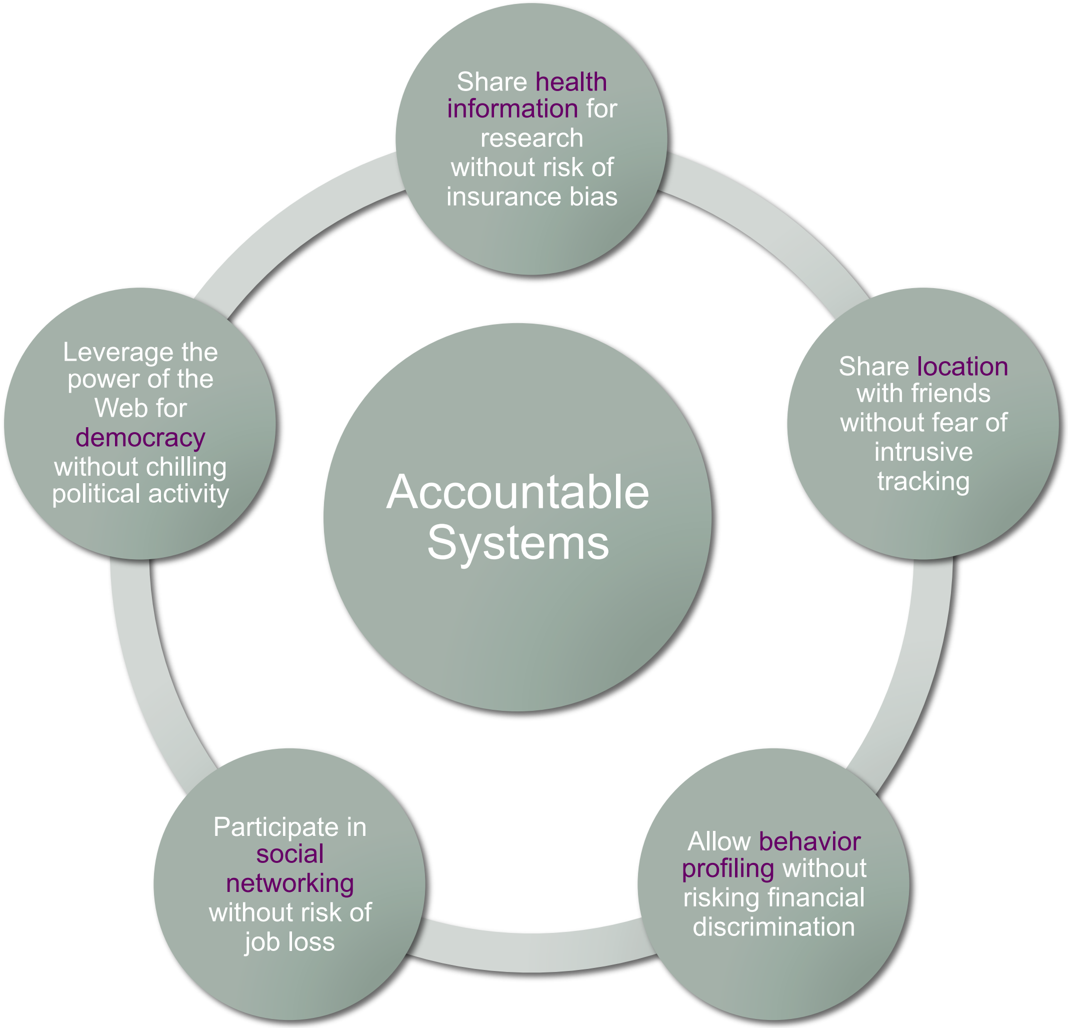
Non-compliance
- FCRA #
- DAA #
- FISA #
- ECPA #

Total Transactions

Net Accountability

Public Trust

The world with Accountable Systems



Accountable Systems

Share health information for research without risk of insurance bias

Share location with friends without fear of intrusive tracking

Allow behavior profiling without risking financial discrimination

Participate in social networking without risk of job loss

Leverage the power of the Web for democracy without chilling political activity

References

- Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, Sussman, Information Accountability, *Communications of the ACM, Jun. 2008, 82-87.*
- 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
- C. Hanson, L. Kagal, D. Weitzner, "Integrated Policy Explanations via Dependency Tracking" (IEEE Policy 2008)
- Pato et all, Aintno: Demonstration of Information Accountability on the Web, Third IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT 2011)
- A. Khandelwal, J. Bao, L. Kagal, I Jacobi, L. Ding, J. Hendler, Analyzing the AIR Language: A Semantic Web (Production) Rule Language 2010
- Waterman and Wang, Prototyping Fusion Center Information Sharing; Implementing Policy Reasoning Over Cross-Jurisdictional Data Transactions Occurring in a Decentralized Environment, IEEE Conference on Homeland Security Technologies (IEEE HST 2010)
- Senevirante, Augmenting the Web with Accountability, World Wide Web Conference 2012 PhD Symposium, April 2012
- Second International Workshop on Accountable Systems: Science, Technology and Policy. http://dig.csail.mit.edu/2014/AccountableSystems2014/
- For more: http://dig.csail.mit.edu/

Work supported by National Science Foundation grant CNS-0831442 CT-M: Theory and Practice of Accountable Systems, IARPA Policy Assurance for Private Information Retrieval grant FA8750-07-2-0031 and the Department of Homeland Security Accountable Information Systems grant N66001-12-C-0082.