

Transparent Accountable Data Mining: New Strategies for Privacy Protection

Deborah L. McGuinness

Co-Director and Senior Research Scientist
Knowledge Systems, AI Laboratory, Stanford

Daniel J. Weitzner

Decentralized Information Group, MIT

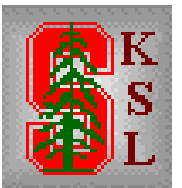
Joint work with: Hal Abelson, Tim Berners-Lee, Chris Hanson, Lalana Kagal, Gerald Sussman, K. Krasnow Waterman



Semantic Web Meets E-Government



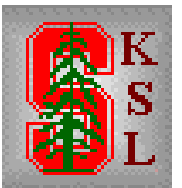
March 28, 2006



Overview

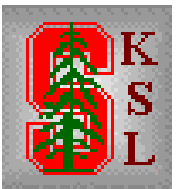
- **General Project Goals**
- **Privacy Policy Intuitions**
- **Motivating Use Cases**
- **TAMI Technical Architecture**
- **Current Implementation Experience**

Funded under NSF's Cybertrust Program



Project Motivation

- **Overall Ambition:** Explore privacy implications of semantic web technologies and determine viability.
- **Goal:** Assess applicability of a usage limitation model (as opposed to or in addition to a data collection model) to data mining/profiling applications.
- Explore technical challenges of provable accountability with explicit justifications in large scale, heterogeneous information systems (i.e., the Web).
- Develop public policy models to encourage transparent, accountable data mining
- **Use case: government data mining applications for terrorism/national security**



Privacy Design Intuition

As more online data becomes available and as inference and interoperability increases, privacy protection will have to rely more on *usage limitation rules* and less on *collection limitation rules*

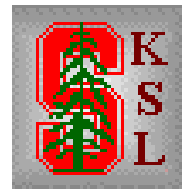
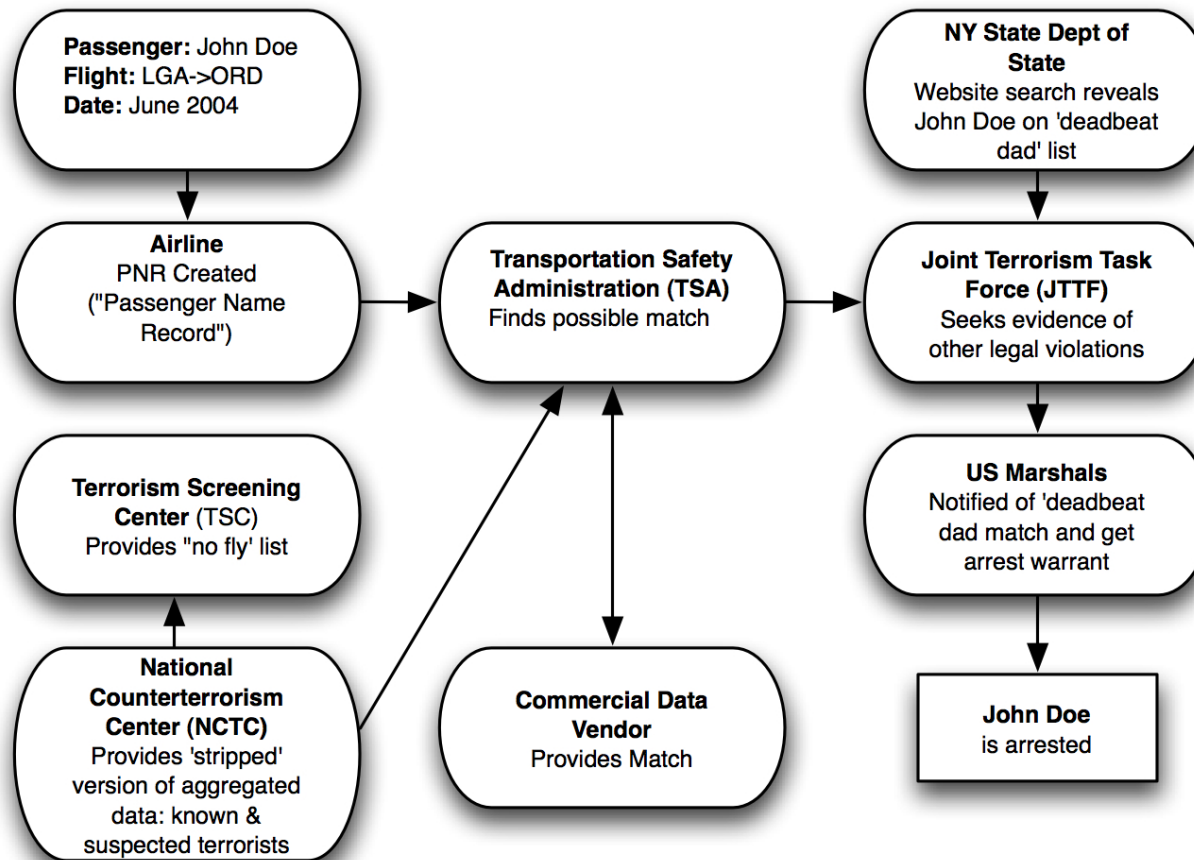
Usage Limits depend upon:

- **Transparency:** knowledge provenance history of sources, data manipulations, and inferences is maintained in an interoperable form. Explanation technology used to allow examination of knowledge provenance by authorized parties (who may be the general public).
- **Accountability:** ability to check whether the policies that govern data manipulations and inferences were in fact adhered to.



Data mining use case

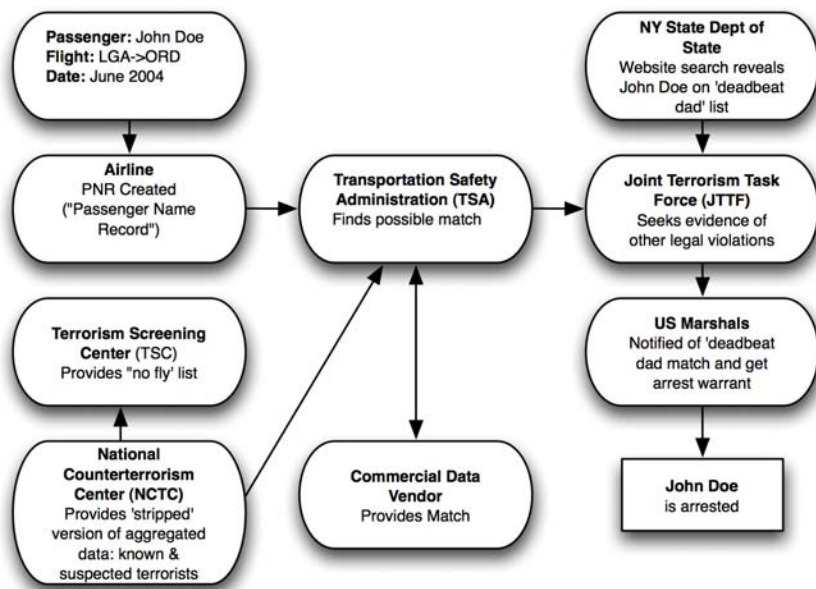
TSA Passenger Screening



Privacy failure modes

- **Errors in matching with lack of transparency**
 - Wrong John Doe (e.g., incorrect address)
- **Improper sharing**
 - No sharing allowed without assertion of 'reasonable suspicion' that there is a national security threat
- **Lack of accountability to rules**
 - TSA collected data under the rule that it only be used for national security investigations

TSA Passenger Screening



Privacy Act


US CODE: Title 5, 552a. Records maintained on individuals - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin Mail Print Address Book Favorites

Address http://www4.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html Go Links >>


Google Search 4 blocked Check AutoLink AutoFill Options

 Cornell Law School Search Cornell

LII / Legal Information Institute home about sitemap donate

U.S. Code collection

main page faq index search



[TITLE 5](#) > [PART I](#) > [CHAPTER 5](#) > [SUBCHAPTER II](#) > § 552a [Prev](#) | [Next](#)

§ 552a. Records maintained on individuals

Release date: 2005-05-18

(a) **Definitions.**— For purposes of this section—

- (1) the term “agency” means agency as defined in section 552 (e) ^[1] of this title;
- (2) the term “individual” means a citizen of the United States or an alien lawfully admitted for permanent residence;
- (3) the term “maintain” includes maintain, collect, use, or disseminate;
- (4) the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Search this title:

Search Title 5

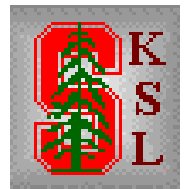
[Notes](#)
[Updates](#)
[Parallel authorities \(CFR\)](#)
[Your comments](#)

Internet



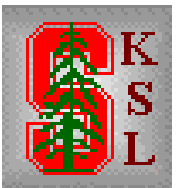
Sharing Restrictions

- (b) Conditions of Disclosure.—
 - No agency shall disclose any record which is contained in a system of records
 - by any means of communication to any person or agency
 - ...
 - except . . . with the prior written consent of, the individual to whom the record pertains,
 - unless disclosure of the record would be—
 -
 - **(3)** for a routine use [5 USC § 552a(b)(3)]

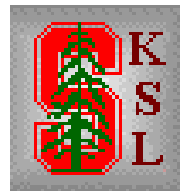
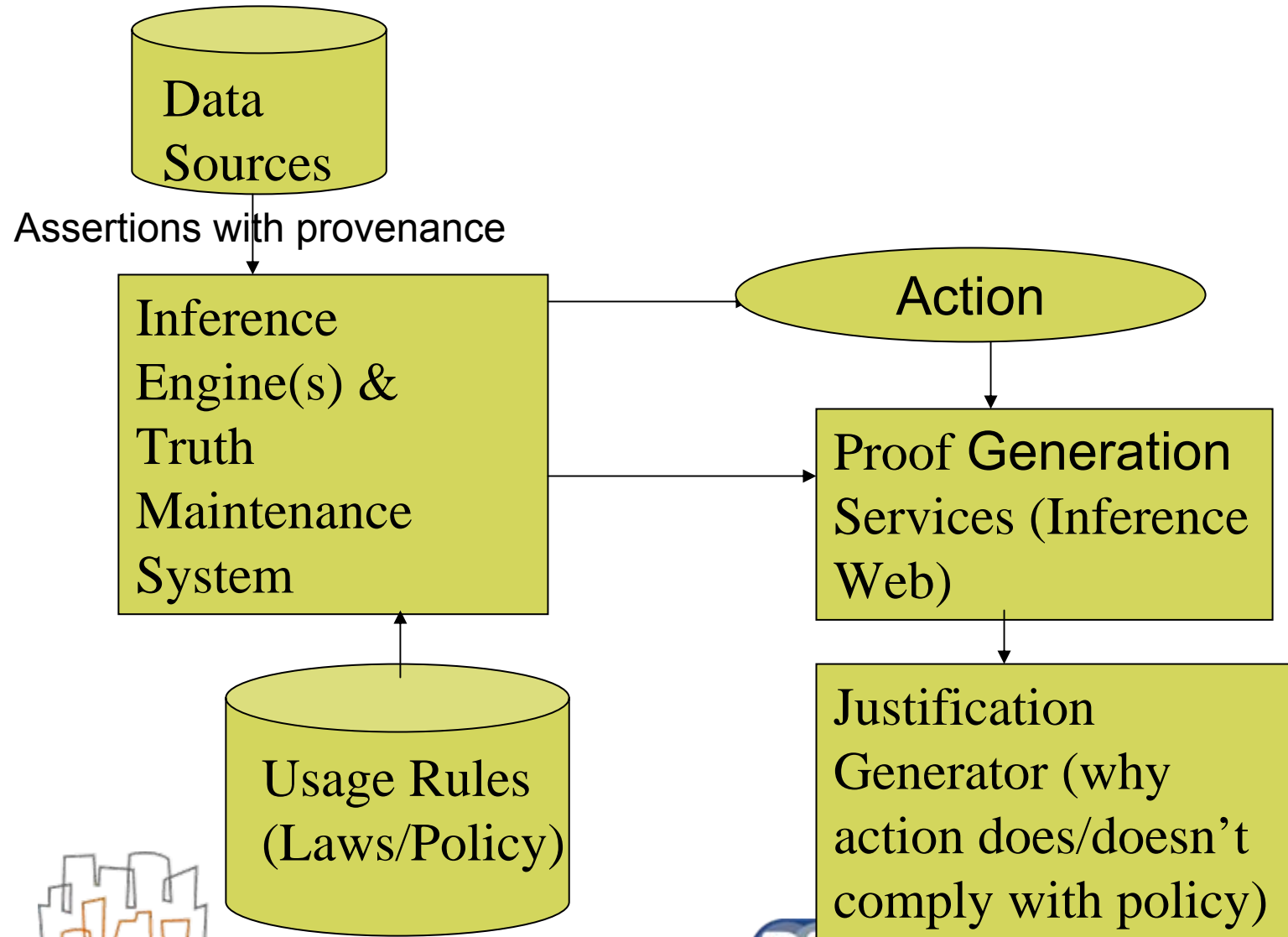


Routine Use

- **as defined in subsection (a)(7)**
 - “the use of such record for a purpose which is compatible with the purpose for which it was collected;” [5 USC § 552a(a)(7)]
- **described under subsection (e)(4)(D)**
 - “publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include—” [5 USC § 552a(e)(4)]
 - “each routine use of the records contained in the system, including the categories of users and the purpose of such use” [5 USC § 552a(e)(4)(d)]



TAMI Architecture



One Simple Description

a ROUTINE USE

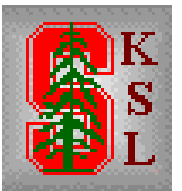
a SHARING_PERMISSION

Recipient : [1,∞] Organization
HasDataCategory : DataCategory
HasPurpose : AuthorizedPurpose

...

General Categories

Structured
Components



Sample Code

RU1 a RoutineUse

; recipient FBI

; category DataCategory3

; purpose CounterTerrorism

Can share with FBI

Data about possible terrorists

So they can investigate whether a criminal law has been violated

; dc:description "May share where TSA becomes aware of information that may be related to an individual identified in the TSDB."

DataCategory3 a DataCategory

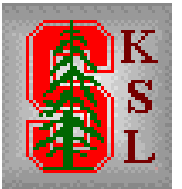
; dc:description "Information about people who are known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."



Inference Web

Framework for *explaining* question answering tasks by abstracting, storing, exchanging, combining, annotating, filtering, segmenting, comparing, and rendering proofs and proof fragments provided by question answerers

- ***Proof Markup Language (PML)***: interlingua for proof interchange with OWL encoding and IW validator service.
- ***IWBase***: distributed repository of meta-information related to proofs and their explanations. Includes services for automatic registration of sources, proof checking, etc.
- ***IW Browser***: displays PML documents containing proofs and explanations (possibly from multiple inference engines)
- ***IW Abstractor/Explainer***: provides multi-modal dialogue options including alternative strategies for presenting explanations, visualizations, abstractions, and summaries
- ***IW Search***: provides search services for PML using SWOOGLE
- ***IW Trust***: provides trust propagation and displays of trust information

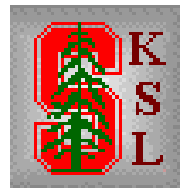


Proof Markup Language Output

```
<rdf:Description rdf:ID="pf455">
  <rdf:type rdf:resource="http://www.w3.org/2000/10/swap/reason#Conjunction"/>
  <rdf:type rdf:resource="http://www.w3.org/2000/10/swap/reason#Proof"/>
  <hasInferenceEngine
rdf:resource="http://inferenceweb.stanford.edu/registry/IE/CWM.owl#CWM"/>
  <pr:component rdf:parseType="Resource">
    <rdf:type rdf:resource="http://www.w3.org/2000/10/swap/reason#Inference"/>
    <hasAntecedent rdf:parseType="Resource">
      <rdf:type rdf:resource="http://inferenceweb.stanford.edu/2004/07/iw.owl#NodeSet"/>
      <hasConclusion> @prefix : &#60;file:/home/connolly/dig-
svn/REPOS/TAMI/2006/03/tami-pf.n3#&#62; .
    @prefix log: &#60;http://www.w3.org/2000/10/swap/log#&#62; .
```

```
:transfer-1a log:outputString ""Legal transfer
on 2005-09-17
from Transportation Security Administration
to Federal Bureau of Investigation
```

```
</hasConclusion>
```



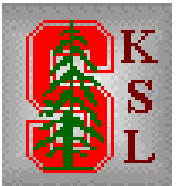
Calculations...

```
<InferenceStep rdf:nodeID="b4">
  <rdf:type rdf:resource="http://www.w3.org/2000/10/swap/reason#Extraction"/>
  <rule rdf:resource="http://www.w3.org/2000/10/swap/reason#Extraction"/>
  <pr:because rdf:parseType="Resource">
    <rdf:type rdf:resource="http://www.w3.org/2000/10/swap/reason#Inference"/>
    <hasAntecedent rdf:parseType="Resource">
      <rdf:type rdf:resource="http://inferenceweb.stanford.edu/2004/07/iw.owl#NodeSet"/>
      <hasConclusion> @prefix : &#60;file:/home/connolly/dig-svn/REPOS/TAMI/2006/03/tami-
pf.n3&#62; .
:SFDB :routineUse :RU1 .
    </hasConclusion>
  <hasLanguage rdf:resource="http://www.w3.org/2004/06/rei#N3"/>
    <isConsequentOf rdf:nodeID="b5"/>
    <s:label>@@evidence</s:label>
  </hasAntecedent>
  <hasAntecedent rdf:parseType="Resource">
    <rdf:type rdf:resource="http://inferenceweb.stanford.edu/2004/07/iw.owl#NodeSet"/>
    <hasConclusion> @prefix : &#60;file:/home/connolly/dig-svn/REPOS/TAMI/2006/03/tami-
pf.n3&#62; .
:RU1 :purpose :CounterTerrorism .
  </hasConclusion>
```



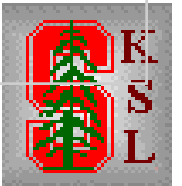
Explanation

- **Why was data sharing xyz acceptable?**
 - Using RoutineUse459
 - We shared with the FBI
 - Data belonging to DataCategory3
 - For the purpose of CounterterrorismCriminalLawEnforcement
 - Provenance: RoutineUse459 is derived from
 - SORN for “Secure Flight”
 - Published at 70 FR 36319
 - Encoded by DHS Office of the Privacy Officer



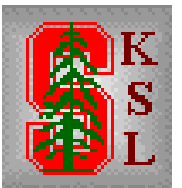
Explanation

- **Why was data sharing xyz *unacceptable*?**
 - We checked all of the RoutineUses
 - We shared with the IRS
 - Data belonging to DataCategory3
 - **IRS is not authorized to receive DataCategory3**
 - For the purpose of CounterterrorismCriminalLawEnforcement
 - Provenance: all RoutineUses are derived from
 - SORN for “Secure Flight”
 - Published at 70 FR 3620
 - Encoded by DHS Office of the Privacy Officer



Discussion

- **Semantic Web technologies can be used to support privacy**
- **We are exploring an explainable usage limitation model**
- **Status:**
 - Use case written up,
 - Project description published,
 - Early prototype in place,
 - Work in progress on reasoning, explanation, integration



More Information

- MIT: Decentralized Information Group - <http://dig.csail.mit.edu/>
- Stanford Inference Web Pages - <http://iw.stanford.edu/>
- Transparency and Accountability - <http://dig.csail.mit.edu/TAMI>
- Policy-Aware Access Control <http://www.policyawareweb.org/>

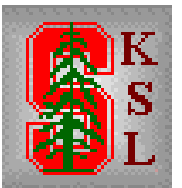
Weitzner, Abelson, Berners-Lee, Hanson, Hendler, Kagal, McGuinness, Sussman, Waterman. Transparent Accountable Inferencing for Privacy Risk Management. AAAI SSS [The Semantic Web meets eGovernment](http://www.ksl.stanford.edu/people/dlm/papers/egov-tami-abstract.html). Stanford, USA 2006. www.ksl.stanford.edu/people/dlm/papers/egov-tami-abstract.html

McGuinness and Pinheiro da Silva. Explaining Answers from the Semantic Web: The Inference Web Approach. Journal of Web Semantics. 1(4). Oct. 2004. www.ksl.stanford.edu/KSL_Abstracts/KSL-04-03.html

Weitzner, Hendler, Berners-Lee, Connolly, "Creating the Policy-Aware Web: Discretionary, Rules-based Access for the World Wide Web." In Elena Ferrari and Bhavani Thuraisingham, editors, Web and Information Security. IOS Press, 2005. <http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf>



Extras



Semantic Web Layers

Ontology Level

- Languages (CLASSIC, DAML-ONT, DAML+OIL, OWL, ...)
- Environments (FindUR, Chimaera, OntoBuilder/Server, Sandpiper ...)
- Standards (NAPLPS, ..., W3C's WebOnt, W3C's Semantic Web Best Practices, EU/US Joint Committee, OMG ODM, ...)

Rules

- SWRL (previously CLASSIC Rules, ...)

Logic

- Description Logics

Proof

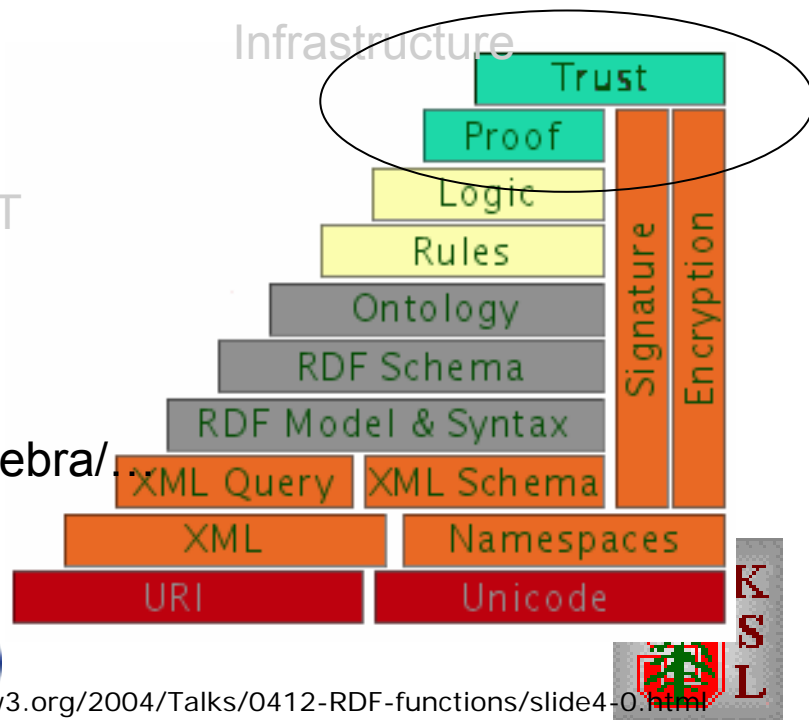
- PML, Inference Web Services and

Trust

- IWTrust, Collaborative Information Repository Trust, NSF TAMI with W3C/MIT

Applications

- VSTO, SESDI, SKIF, SSOA, BISTI, ...
- Domain ontologies & environments
- Tools academic & industry – sandpiper/cerebra/



Sample Code (Second Formalism Style)

- **(sorn:Routine-use #f**

- sorn:recipient te:FBI
- sorn:category :data-category-3
- sorn:purpose te:ct-criminal-law-enforcement
- dc:description
 - " May share where TSA becomes aware of information that may be related to an individual identified in the TSDB.")

Can share with FBI

Data about possible terrorists

So they can investigate whether a criminal law has been violated

- **(sorn:Data-category :data-category-3**

- dc:description
 - " Information about people who are known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism."



General Nature of Descriptions

a SOR

a DATA_REPOSITORY

hasControl: ExecBrnchFedGov [= 1]

hasRecord: [>= 1] USPerson

A USPerson =
(OR USCitizen LegalPermRes)

General Categories

Structured
Components

“Data repository held or controlled by the executive branch of the federal govt. It contains information about a US Citizen or a legal permanent resident”

