Transparency and Accountability

Motivating the Policy Aware Web

Daniel J. Weitzner djweitzner@csail.mit.edu
MIT Computer Science and Artificial Intelligence Laboratory
Decentralized Information Group

Motivating the Policy Aware Web

- Privacy and Security Challenges
  - Case studies
  - Larger trends
- Inadequacy of current legal and technical tools
- Way forward: Embrace transparency and require accountability
- What is the Policy Aware Web?

Privacy, Security and Transparency Challenges

- Law Enforcement
- Large-scale Data mining
- Database Security

Current inferencing limits: DC Sniper Investigation

"Authorities in the Washington region spotted the same faded blue 1990 Chevrolet Caprice and recorded its New Jersey tags on at least 10 different occasions this month....

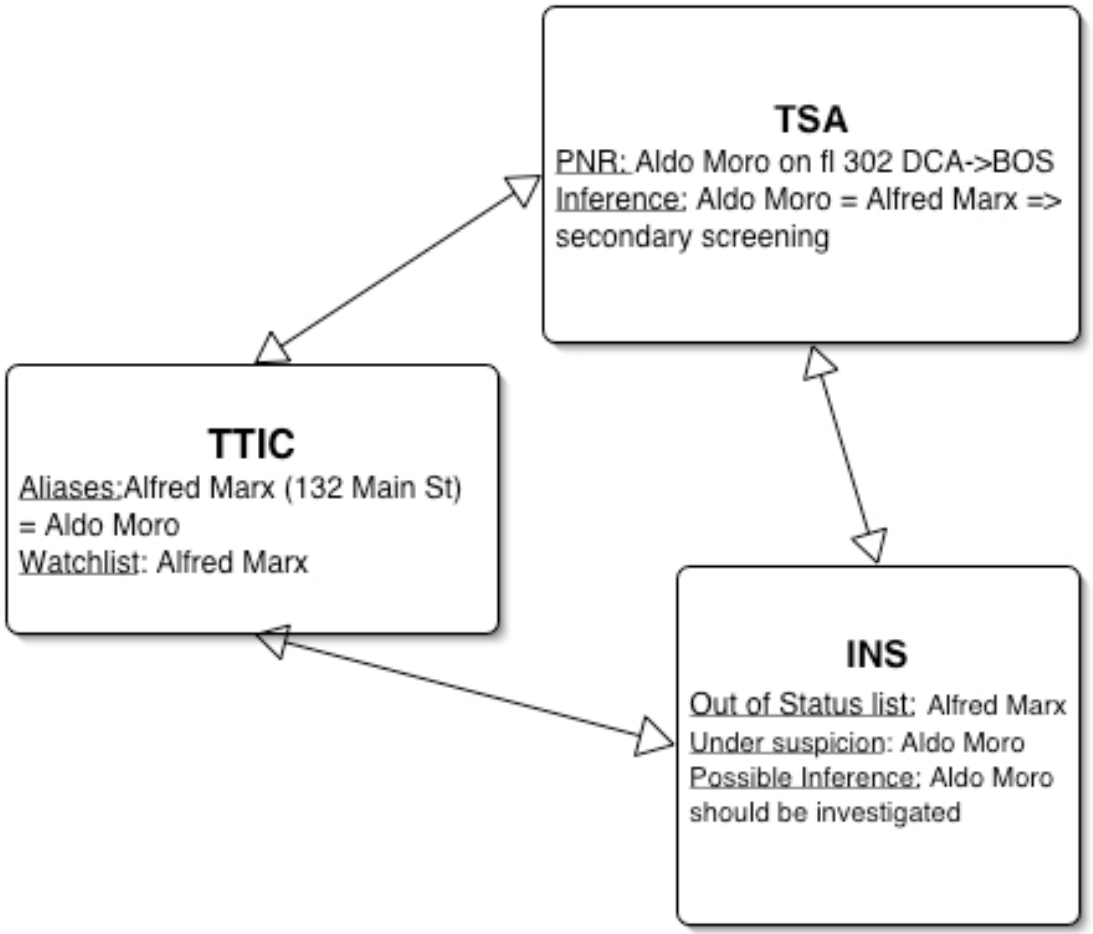
Each time, however, they let the driver go after finding no record that it had been stolen or that its occupants were wanted for any crimes.

Washington Post 26 October 2002, p.A01

'We were looking for a white van with white people, and we ended up with a blue car with black people,' said D.C. Police Chief Charles H. Ramsey"

CSAIL

Large-scale datamining (for airline security)



CSAIL

Database Leaks

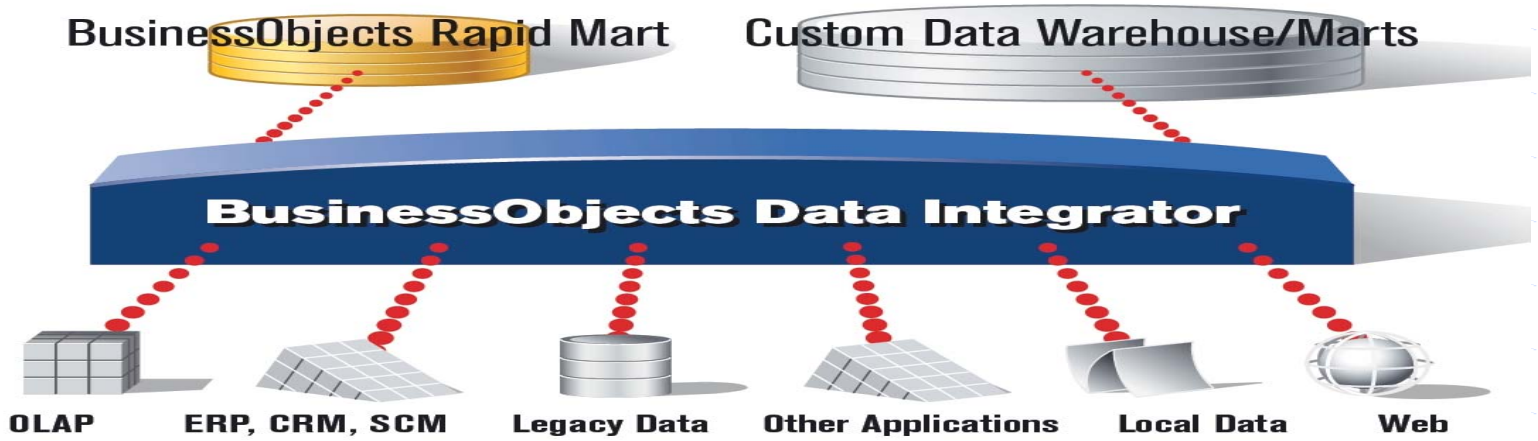
- Choicepoint: access allowed for unauthorized persons
- Lexis-Nexis: data loss
- Iron Mountain: lost tape of plain-text personel records

CSAIL

Larger technical trends toward transparency

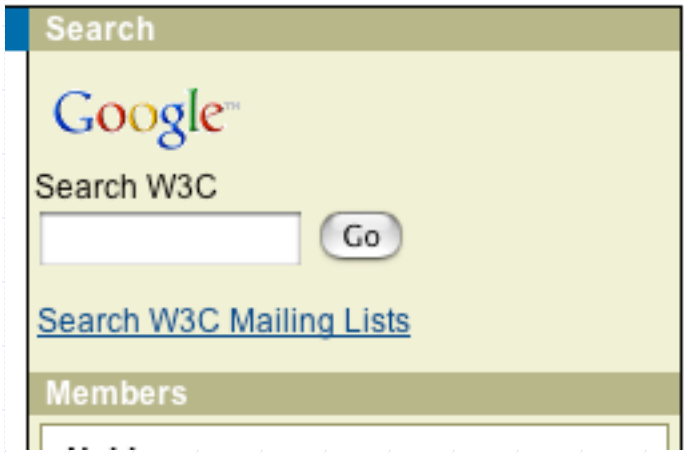
- The end of ‘stovepipes’
- Cheap query
- Location-aware sensor nets
- Cost of storage = zero

1. The End of ‘Stovepipes’



CSAIL

2. Cheap query: institution-wide and Web-wide



CSAIL

3. Location-aware Sensor Nets

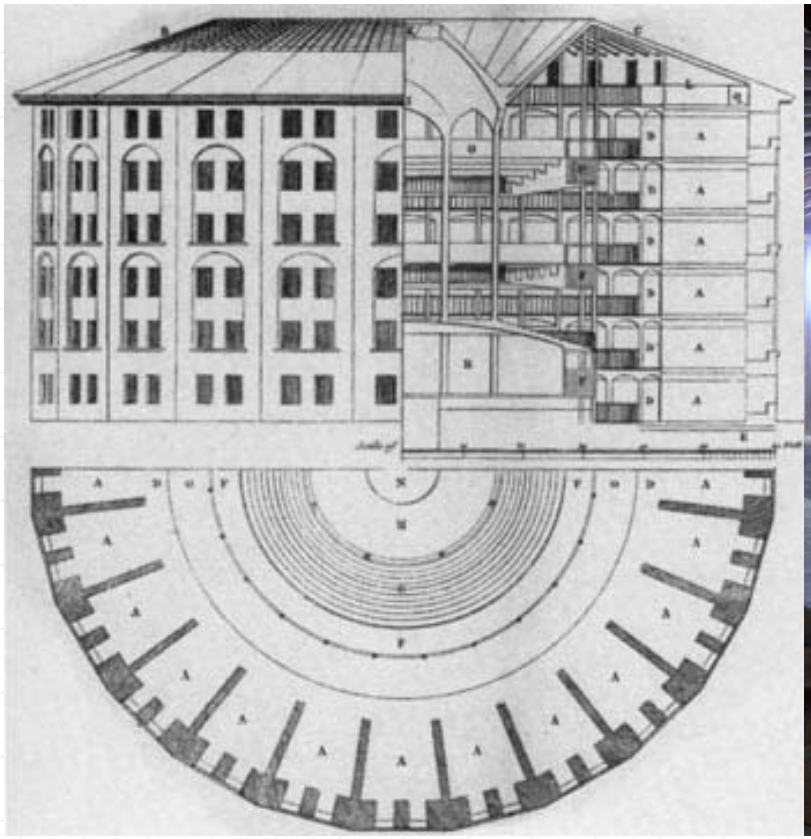
CSAIL

4.Cost of Storage approaches zero

You are currently using 0 MB (0%) of your 1000 MB.
Terms of Use - Privacy Policy - Program Policies - Google Home
©2004 Google

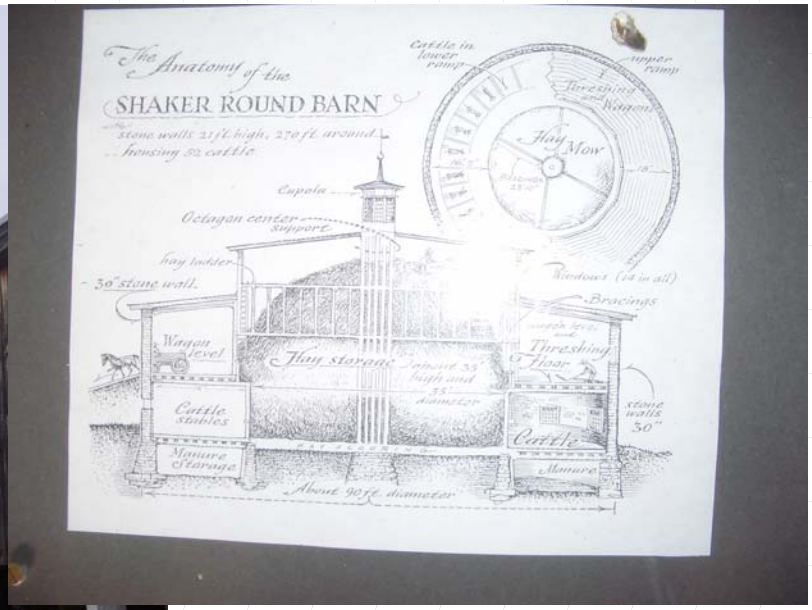
CSAIL

Avoiding Technological Determinism



CSAIL

And Avoiding Policy Formalism



CSAIL

Challenge to existing privacy model: from evidence to inference

Most intrusive practices are from inferences drawn, not evidence collected:

- Credit card transactions → profiling
- Web logs → Web search patterns
- Instantaneous location → travel patterns

Current Legal Tools to address inferencing power

- US Const. Fourth amendment
- Wiretap laws
- EU Data Protection Directive
- However, neither the Fourth Amendment nor wiretapping statutes impose any *limits on what the government can do with information once it has been collected*.

Current technical tools to address inferencing power

- Anonymity and de-identification: but see Sweeney
- “Privacy-preserving” data mining through Secure Multiparty Computation: but consider leaks in real-world application

Managing Transparency With Accountability

- Apply accountability techniques to
  - Law enforcement data collection
  - Large scale data mining
  - Security policy audit
- Policy Aware Technology is *Necessary but not Sufficient*
- Public Policy agenda: facilitate accountability
  - from collection limits to usage rules
  - Enforcement of agreements

Living with the Transparency Paradox

"Assume the (unauthorized) user knows all ciphering procedures"

-Kerckhoffs' Principle (1835-1903)

The transparency paradox: that we may have to embrace greater exposure of personal information in order to advance fundamental privacy values.