Information Accountability: A New Approach to Privacy in Data Mining

National Science Foundation
Symposium on Next Generation of Data Mining and Cyber-Enabled Discovery for Innovation
10 October 2007

Daniel J. Weitzner <djweitzner@csail.mit.edu>
MIT Decentralized Information Group

Supported by NSF ITR (04-012), Cybertrust (05-518)
Overview

• Current privacy challenges
• Poor fit with current technical and legal approaches
• Information Accountability as an alternative model for privacy in large (Web) scale information analytics
Changing Views 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 others.*
Persistent Privacy Problems for Data Mining Applications

The pilot programs ignored privacy safeguards, says a recent Homeland Security report.

By Mark Clastrier, Staff Writer of The Christian Science Monitor

From late 2004 until mid-2006, a little-known data-mining computer system was used by the Homeland Security to hunt terrorists, weapons of mass destruction, and Americans' personal data with little regard for federal privacy laws.

Now the $42 million cutting-edge system, designed to process trillions of data points every day, has been canceled pending data-privacy reviews, according to a new report by the Department of Homeland Security. The DHS operates at least a dozen such programs, and the Department of Defense employs many others.

Data mining to help fight the war on terror has become an accepted technique for analyzing and interpreting data. But the DHS's Analysis, Dissemination, Visualization, Insight, and Segregation (ADVICE) program, which was designed to analyze e-mail traffic, intelligence reports, and other sources, has raised serious privacy concerns.

Sifting through enormous volume of information at lightning speed, ADVICE was to displace and simplify -- a sort of illuminated information constellation -- in which the system's pilot programs used "live data, including multiple sources in attempts to identify potential terrorist activity," to quote the DHS's own internal guidelines to keep that data from being released.

Report: DHS didn't follow guidelines

Yet ADVICE, whose existence and scope were limited by the agency's own ambitious scope, failed to incorporate federal guidelines in its earliest days. The system's pilot programs used "live data, including multiple sources in attempts to identify potential terrorist activity," by law and DHS's own internal guidelines to keep that data from being released. General (OIG) said in a June report to Congress, which was made public.

House committee chair wants in on DHS data-mining programs

Jalalpur Vijayan, September 18, 2007 (Computerworld) Bennie Thompson (D-Miss.) said in a letter to Homeland Security Secretary Michael Chertoff that he had asked the Department of Homeland Security's Privacy Office to look into the details of all the programs that have been canceled, including ADVICE. He also asked for details on the amount of money the DHS spent on contractors who were awarded funds and for an explanation of the projects and information about privacy issues.

Thompson's demand was prompted by the recent cancellation of the ADVICE program, which was shelved because of privacy concerns after $42 million had been spent on it. In a letter to Chertoff yesterday, Thompson expressed concern about the "apparent failure" of DHS programs that have been canceled or otherwise modified after millions of dollars have been spent. He asked for details on the amount of money the DHS spent on contractors who were awarded funds and for an explanation of the projects and information about privacy issues.

DHS officials could not be reached for comment.

By Robert M. Cook

Dr. Deborah Harrigan remembers the day two pharmaceutical company representatives told her she wasn't prescribing enough of a drug they sold.

The Rochester family physician, who was working at the city's Arv Goodman Community Health Center at the time, said she was surprised they knew so much about her prescribing history.

The information comes from data mining companies, which collect, analyze and sell data about the type of prescriptions written by other physicians. The techniques aren't without controversy — Harrigan, for example, said she believes doctors at least should be told if their data is being collected and sold. That isn't now required.
Current Approaches

• Legal rules fail to address new privacy challenges
• "Privacy preserving data mining" techniques fail at scale and over time
Legal Limitations

Most intrusive practices are from inferences drawn, not individual quanta of information collected:

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

Most laws impose *collection* barriers:

- Wiretapping
- Data breach laws
Technical Limitations

*When Privacy Sensitive Data Analysis succeeds, are we done?*

- A privacy-safe zone: Privacy sensitive data mining establishes a boundary, which, if respected, assures no privacy risk to the individual.

- How do you know that data usage remains within the privacy-safe zone:
  - over time?
  - across an institution?
  - across the Web?

- What legal rules outside the privacy-safe zone?
How can we protect the privacy in increasingly transparent information environments?
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 be possible to determine what happened, and to pinpoint use that is inappropriate.
Information Accountability as an alternative to secrecy

• Rules and law should govern how information is used: "It is illegal to consider health status of applicant or her family in hiring decisions"

• Interactions with data are logged in order to provide possibility of machine-assisted human-driven accountability
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 penalties for failure to file
  - virtually no review of substance of reports unless some stops trouble
  - criminal penalty for misreporting
Accountability architecture

- Access control through Decentralized Authentication Proofs based on access rules expressed over data semantics
- *Transparent* data usage logging for real-time compliance hints and *a posteriori* accountability
- Engineered as Web architecture components

Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, Sussman
Information Accountability, 2007
AIR: An RDF Policy Language for Usage Rules

:Rule1 a air:Belief-rule;
  air:variable :U2;
  air:variable :P2;
  air:variable :AP;
  air:label "FirstAIRRule";
  air:pattern
  {
    :U2 a air:UseEvent;
    :refers-to [ a mit:ProxCardEvent ];
    :purpose P2;
    :UseEvent :allowed-purposes :AP.
    :P2 is-member-of :AP
  };
  air:assert { :U2 :validPurpose :P2 }.
Research Questions

- What kind of language should be used to express information usage rules?
- What tools and techniques will help encourage rule-following and spot non-compliance?
- Can we apply statistically-based anomaly detection and pattern recognition to spot privacy intrusions?
- What kinds of legal systems will encourage the development of accountable information systems?
For More Information

- Feigenbaum and Weitzner (eds.), "*Report on the 2006 TAMI/Portia Workshop on Privacy and Accountability.*"