

# **Granular Access: Information Sharing in a World of Complex Laws & Policies**

Presented to the Collaborative Expedition Workshop  
At the National Science Foundation  
By K. Krasnow Waterman  
November 8, 2005

# K. Krasnow Waterman

K. Krasnow Waterman is a lawyer and technologist who has worked in private industry and government. Since 9/11 her work has focused on the combination of the two professions. Ms. Waterman was the first Chief Information Officer of the Foreign Terrorist Tracking Task Force and, later, Acting Section Chief for Intelligence Capabilities of the FBI's new Office of Intelligence. More recently, she has served as a senior policy advisor to the DHS Information Sharing and Collaboration Office. She is now a Sloan Fellow at the Massachusetts Institute of Technology.

This presentation is available at: [www.kkrasnowwaterman.com](http://www.kkrasnowwaterman.com)

# Historical Perspective

- Access
  - Paper file
  - Computer record
  - Data element
- Sharing
  - Data dump
  - Data warehouse
  - Access on demand

# Two Current Projects

- Information Sharing Environment
  - Executive Order 13388
  - Intelligence Reform & Terrorism Prevention Act of 2004 (section 1016)
- National Health Information Network
  - <http://www.hhs.gov/healthit/nhin.html>

# What do we want to do?

- All the things we've done before
  - Publish
  - Subscribe
  - Create user accounts
  - Search documents
- Ask a narrow question. Get a narrow answer.
  - Has the patient ever taken Paxil before?
    - "10/16/2001"
  - Does Osama Bin Laden have a sister named Azzam?
    - "No information found"

# Common Themes

- Decentralized
- Web architecture
- Shared standards
- Individual implementation
- Governance
- Enhanced security
- Enhanced privacy
- Inclusiveness

# Why?

- Improve
  - Accuracy
  - Security
  - Speed
  - Coordination
  - Collaboration
  - Flexibility

**HOW?**



# Requirements

- Identity management
- Access control
- Granular search
- Federated query
- Comprehensive audit

# Identity Management

- Who are you?
  - Name
  - Employer
  - Title
  - Clearances
- What are you doing?
  - Duty at that moment
- Technical requirements:
  - Enhanced user metadata
  - Dynamic link to human resources data

# Access Control

- Which business rules apply to accessing this data?
  - Can this category of person doing this category of work have access to the data requested?
  - What rules does this person's organization have about sharing that should affect my decision?
- Technical requirement:
  - Means to create a non-hierarchical rules library
  - Means to determine rules hierarchy for the particular request
  - Rules engine to apply the rules to the identity and work activity data
  - Dial up/down access control

# Granular search

- Ability to determine if the repository has the discrete fact sought
- Ability to perform statistical searches
- Ability to perform non-repetitive queries
- Technical requirements:
  - Search algorithms
  - Entity extraction
  - Fuzzy matching
  - Data harmonization
  - Anonymization

# Federated Query

- One query to multiple repositories
- Technical requirements:
  - Secure connections
  - Middleware
  - Means for addressing data in repositories without data dictionaries
  - Context mediation

# Comprehensive Audit

- Ability to address internal, legal, and public queries
- Technical requirements:
  - Transactions logged per data element
  - Dynamic matching of access patterns to statistical norms

# Exploring the business rules of government

How much impact will they have on architecture and implementation?

# What are “Business Rules” that apply to information sharing?

- Legal Authorities
- Community of Interest Rules
- Agency Policies
- Stakeholder Policies
- Professional Standards
- Other



# How many “Business Rules” are in each of these areas?

- Hundreds? Thousands?
  - For example, legal authorities include:
    - Statutes
    - Executive Orders
    - Presidential Directives
    - Federal Regulations
    - Court Decisions
    - Other

# How many Communities of Interest create “Business Rules”?

- Hundreds?
  - Intel
  - Law Enforcement
  - Health
  - Physical Security
  - Systems Security
  - Privacy
  - Civil Liberties
  - Technical
  - Other

# How hard are they to find?

- Rules often don't use "keywords"
  - Criminal – grand jury, exculpatory evidence
  - Attorney-client privilege
- Or "keywords" are common words
  - Share, transfer, disclose, etc.

# How complex is a single "Business Rule"?

- **Varies**

- One rule can

- Require understanding of a characteristic of a database (including those that will change)
    - Require links to other databases
    - Require information about the employer of the requestor
    - Require information about the job of the requestor
    - Require information about the task of the requestor
    - Have requirements that are consistent and requirements that are variable
    - Change!

# Example: The Privacy Act

- Has 29 possible decisions
- Is partly
  - Applicable in the same manner to all
  - Interpreted differently and applied differently
  - Totally at the discretion of the individual agency per data repository

# Prior projects

- Information Sharing Agreement Matrix
  - 50 most common questions
  - The people who answer them
  - The people who validate the answers
- Rules ontologies
- Parsed rules (decision trees)
- Deconstructed Routine Use notices

# Ongoing projects

- Shifting from “need to know” to “share at the first point of usability”
- Redefining tear-lines
- Re-examining third party rules

# Design decisions

- Incremental implementation
  - Room to grow
  - Plans to change
- Identity Management & Access Control  
(The Lock & Key)
- Access Granted or Data Searched  
(The Chicken or The Egg)
- Centralized or decentralized
- Common standards or translation tables
- Institutional trust or personal trust



# Policy Issues

- Existing laws anticipate file-based sharing
- Current rules value original source of information over authority of requestor
- Electronic implementation of rules is likely to create system lock-outs
- FOIA expects holder of data to always be able to identify federal agency source

**Questions?**