

Privacy and Policy Session

The 2006 Biometric Consortium Conference
Baltimore Convention Center
Tuesday, September 19th 2006, 2:00 p.m. - 3:00 p.m.



Homeland Security

The Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
t: 571-227-3813; f: 571-227-4171
privacy@dhs.gov; www.dhs.gov/privacy

Overview

Purpose: Different perspectives of "Privacy"

Panelists:

- Peter E. Sand: Conceptual Framework
Director of Privacy Technology, DHS Privacy Office
- Ari Schwartz: Privacy Advocacy
Deputy Director, Center for Democracy & Technology
- Brandon J. Schneider: Legal Considerations
Senior Legal/Policy Consultant, DoD Biometrics Task Force

Questions & Answers



Homeland Security

The DHS Privacy Office
October 6, 2006: slide 2

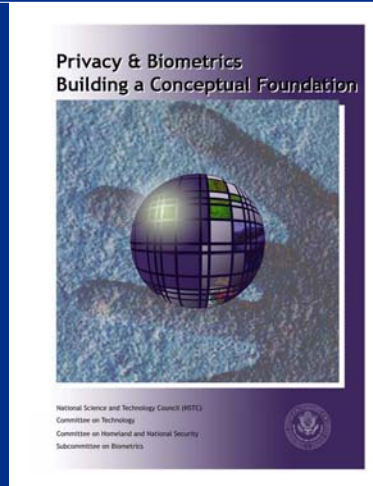
Focused Effort

NSTC Paper

- Overview of Technology
- Overview of Privacy
- "Functional Architecture"
- Integration

Operational Framework

- Within Biometrics...
- Applicable Privacy Issues
- Implementation Guide



Homeland Security

The DHS Privacy Office
October 6, 2006: slide 3

Defining Concepts

Concepts

- Decisions
- Spaces
- Intentions
- Informational

Torts: Private Law Suits

- Interference
- Embarrassment
- Stealing (. . . Copying?)

Constitutional Protections

- Anonymity
- Home
- Unreasonable Gov't search/seizure
- Self-Disclosure

Harms: "Taxonomy"

Surveillance	Blackmail
Interrogation	Appropriation
Aggregation	Distortion
Identification	Intrusion
Insecurity	Secondary Use
Exclusion	Decisional Interference
Disclosure	Breach of Confidentiality
Exposure	Increased Accessibility

"A Taxonomy of Privacy" - Daniel J. Solove
Professor of Law, The George Washington University Law School



Homeland Security

The DHS Privacy Office
October 6, 2006: slide 4

Information Privacy: Data

Appropriate Use of Personal Information

ANY Information that COULD
be USED in ANY WAY to IDENTIFY an INDIVIDUAL

- Two ways information can become personal
 - Content: Name, Unique Identifier, sufficient "facts"
 - Intent: Used for the purpose of identifying individual
- Full information life cycle across all uses



**Homeland
Security**

The DHS Privacy Office
October 6, 2006: slide 5

Information Privacy: Use

Appropriate Use

- Founded in Law or sound & legit public policy
- Clearly articulated
- Previously disclosed
- Closely related to purpose of original collection

Throughout entire information life cycle

- As data changes
- As use changes
- As use changes the data
- Information Sharing: full extension
- As technology changes what is possible: "new" info.



**Homeland
Security**

The DHS Privacy Office
October 6, 2006: slide 6

Biometrics Challenge: Privacy

Challenges

1. Fundamental understanding of privacy principles
2. Embed privacy functionality into every layer of the architecture, from the sensor through the system to the interoperable biometrics network.
3. Privacy-protective solutions that meet operational needs, enhance public confidence in biometrics technology and safeguard personal information.

Focus of Research

1. Guidelines for auditing biometrics systems and records
2. Framework for integration of privacy principles in biometrics system design



**Homeland
Security**

The DHS Privacy Office
October 6, 2006: slide 7

Information Privacy: Action

Initial Orientation: First and Always

1. Nature of Technology (*information* technology)
2. Current Status

Within the System/Technology

3. Purpose & Success
4. All Data
5. All Uses
6. All Technology
7. Access, Control & Audit
8. Documentation

Biometrics Architecture

1. Collection
2. Conversion
3. Storage
4. Comparison
5. Decision



**Homeland
Security**

The DHS Privacy Office
October 6, 2006: slide 8