

The Crossroads of Privacy and Biometrics

John W. Kropf
U.S. Department of Homeland Security
Privacy Office

ETHICS AND POLICY OF BIOMETRICS AND
INTERNATIONAL DATA SHARING

Hong Kong Polytechnic University

January 4, 2010



**Homeland
Security**



What is 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.

*Alan Westin, Privacy and Freedom,
Atheneum, New York, 1967, p. 7*



Homeland
Security



Biometrics – Worldwide

- ❑ ICAO: Standard for Passports
- ❑ EU: Passports (ICAO +finger scans)
- ❑ US: US – VISIT; BioVisa
- ❑ Japan: Entry and Exit
- ❑ UK: Borders
- ❑ Israel : Legislation on a National Biometric Data Base
- ❑ UAE: Borders
- ❑ Pakistan: National IDs
- ❑ Registered Traveler Programs (US, The Netherlands, others)
- ❑ Many others



Why Privacy Is Important to Biometrics

- ❑ Fundamental right (UN Convention)
- ❑ Good government
- ❑ Legal compliance
- ❑ Budget implications



Homeland
Security



Overview: U.S. Privacy Framework

- Domestic (USG only not private sector)
 - Privacy Act of 1974
 - Freedom of Information Act (FOIA)
 - E-Government Act of 2002
 - Presidential Orders, Directives and Guidance
- International
 - Information Sharing Agreements
 - International Frameworks



Homeland
Security

Application of the Privacy Act

Information Protected

- Information about an individual containing their name or other personal identifier in a Federal agency record system.
- Examples: education, financial transactions, medical history, criminal history, employment history, digital photographs, fingerprints

Applies to a “system of records” (SORNs)

- Any group of records containing information about U.S. persons
- Under the control of a Federal agency
- AND agency retrieves information by the individual’s name or other personal identifier including biometrics.



**Homeland
Security**



DHS Privacy Office

- New technologies do not erode privacy
- Personal information used in compliance with US law.
 - Laws follow the Fair Information Practice Principles (FIPPs)
- Evaluate new legislation
- Coordinate with DHS Civil Rights and Civil Liberties
- Report to Congress
- Freedom of Information Act



Homeland
Security



Example: US-VISIT and Privacy

- US Congress, through a series of statutes, required the creation of a biometric entry-exit system.
- Resulted in US-VISIT.
- US-VISIT's goals:
 - Enhance the security of U.S. citizens and visitors
 - Facilitate legitimate travel and trade
 - Ensure the integrity of the U.S. immigration system
 - Protect the privacy of visitors.



Example: US-VISIT and Privacy

- ❑ **Transparency:** IDENT PIA and SORN
- ❑ **Minimization:** Collects only the information needed to achieve US-VISIT statutory authority
- ❑ **Use Limitation:** Sharing this information must be consistent with the purpose for which it was collected.
- ❑ **Security and Privacy:** Success of the US-VISIT measured by ability to identify threats but to protect against ID theft and fraud.
- ❑ **Accountability:** US-VISIT PO and DHS CPO; periodic audits
- ❑ **Robust Privacy Policy:** Privacy protections extended to non-U.S. citizens
- ❑ **Access and Redress:** Freedom of Information Act, Privacy Act and TRIP.



SORNs and PIAs are Publicly
Available

<http://www.dhs.gov/privacy>



Biometrics: Critical to Government

- ❑ Lost and Stolen Passports
- ❑ Border Controls
- ❑ Advance Screening



Sharing Biometrics Across Borders

- FIPPs
- Mutual Recognition of Systems
- HLCG Principles



Homeland
Security



Contact Us

U.S. Department of Homeland Security

Privacy Office

Washington, DC 20528-0550

Tel: 1-703-235-0780

Email: privacy@dhs.gov

Website: www.dhs.gov/privacy



Homeland
Security