Biometric Identification: It's Complicated

Melissa Ngo, Esq.

Privacy and Information Policy Consultant

National Defense Industrial Association

National Security through Biometric Collaboration:
A Roadmap to Tomorrow

February 23, 2011

Arlington, Va.

Definition and types

- Automated recognition of an individual based on physical or behavioral characteristics

- Includes scans of finger, iris, face, palm, voice, brain, DNA

Before you begin . . .

Some questions to ask:

- What is the purpose of the system to be created?
- What is the scope of the system?
- Is biometric ID likely to be the best system to reach your goal? Why?
- Do its benefits outweigh implementation, security, and other costs?
- How will you ensure security and privacy of the system?

Complex systems

- Biometric systems can include:
  - Physical parts: Database of biometrics, machinery to scan biometrics for input into database and to query database, people who enter or evaluate the biometric, outside auditors
  - Policy parts: Who has access and when? What if person can't or won't give the required biometric? What happens if there is a false match or false nonmatch? What happens if there is identity theft or fraud?

Problems with biometric-gathering

- Physical problems
- Religious or cultural problems
- Discomfort problems
- Failure to enroll problems could lead to discrimination or disenfranchisement

Privacy concerns

- Covert collection
- Unintended purposes (mission creep)
- Secondary information

Reliability questions

- Systems can be compromised
- Error rates in question
  - False matches/positives;
  - False nonmatches/negatives
- High-profile mistake: Brandon Mayfield case

Lowering privacy and security risks

- How is the system set up, protected, and maintained?
- Stringent security and audit trails
- Outside audits
- Allow people access to their records, remedies
- Limit retention, sharing and purposes