Privacy Issues Associated with Biometrics

Samuel P. Jenkins, Director

Defense Privacy Office, Department of Defense

2010 NDIA Biometrics Conference

January 20-21, 2010

Focus of Today's Presentation

- Fair Information Practices and Principles
- Biometrics and Privacy Best Practices
  - Scope and Capabilities
  - Data Protection
  - User Control of Personal Data
  - Disclosure, Auditing, Accountability, and Oversight

Fair Information Practice Principles

- Transparency – Agencies should provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
- Individual Participation – Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding an agency's use of PII.
- Purpose Specification – Agencies should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- Data Minimization – Agencies should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose.

Fair Information Practice Principles

- Use Limitation – Agencies should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the agency should be for a purpose compatible with the purpose for which the PII was collected.
- Data Quality and Integrity – Agencies should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- Security – Agencies should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing – Agencies should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Biometrics & Privacy Best Practices

Scope and Capabilities

- **Scope Limitation**
- **Establishment of a Universal Unique Identifier**
- **Limited Storage of Biometric Information**
- **Evaluation of Potential System Capabilities**
- **Collection or Storage of Extraneous Information**
- **Storage of Original Biometric Data**

Biometrics & Privacy Best Practices

Data Protection

- **Protection of Biometric Information**
- **Protection of Post-Match Decisions**
- **Limited System Access**
- **Segregation of Biometric Information**
- **System Termination**

Biometrics & Privacy Best Practices

User Control of Personal Data

- **Ability to "Unenroll"**
- **Correction of and Access to Biometric-Related Information**
- **Anonymous Enrollment**

Biometrics & Privacy Best Practices

Disclosure, Auditing, Accountability and Oversight

- **Third Party Accountability, Audit, and Oversight**
- **Full Disclosure of Audit Data**
- **System Purpose Disclosure**
- **Enrollment Disclosure**
- **Matching Disclosure**
- **Use of Biometric Information Disclosure**

Biometrics & Privacy Best Practices

Disclosure, Auditing, Accountability and Oversight (Cont.)

- **Disclosure of Optional/Mandatory Enrollment**
- **Disclosure of Individuals and Entities Responsible for System Operation and Oversight**
- **Disclosure of Enrollment, Verification and Identification Processes**
- **Disclosure of Biometric Information Protection and System Protection**
- **Fallback Disclosure**

Questions