

International·Biometric·Group

R e s e a r c h C o n s u l t i n g I n t e g r a t i o n

Assessing Privacy Risks in Emergent Biometric Systems

Michael Thieme
Director of Special Projects
International Biometric Group

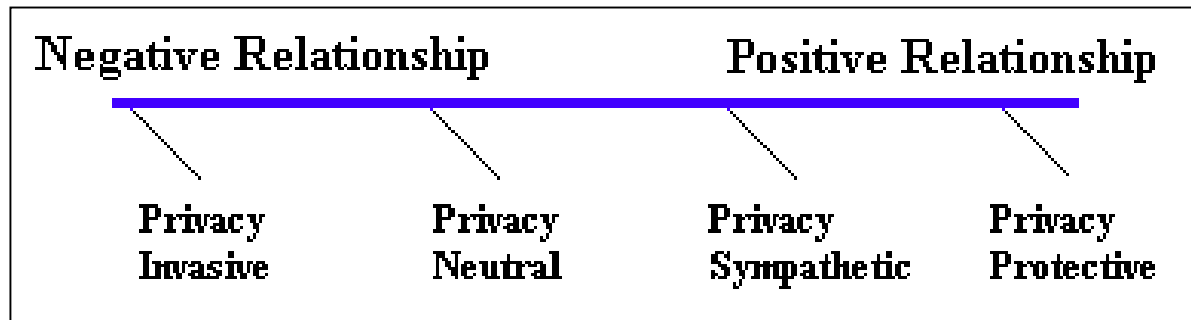
Security & Privacy Conference - Synergies in an e-Society
10-11 February 2005
Victoria, British Columbia

About International Biometric Group

- Independent biometric technology solutions, consulting, and research & testing firm
 - NYC, London, Washington DC; founded 1996
 - Technology-neutral and vendor-independent
- Advise government, commercial entities on large-scale biometric implementations
 - Cost/benefit, migration strategies, standards compliance
- Design and build biometric systems for custom applications
- Evaluate emerging biometric technologies for commercial viability, accuracy

Biometrics on a Privacy Continuum

- *Biometrics' relationship with privacy is multifaceted*
- Privacy protection through biometrics
 - Providing access to sensitive data
 - Allowing individual control over personal information
 - Protecting against identity fraud / theft



- Privacy erosion through biometrics
 - Used for broader purposes than originally intended (linking disparate data, tracking behavior)
 - Captured without informed consent

Evaluating Biometrics/Privacy Relationship

- BioPrivacy Framework
 - Applications – Technologies – Best Practices
- BioPrivacy Application Evaluation
 - Not all biometric deployments bear the same privacy risks: specific features of biometric deployments increase or decrease the likelihood of misuse
- BioPrivacy Technology Risk Ratings
 - Certain technologies are more prone to be misused than others and require extra precautions
- BioPrivacy Best Practices
 - Provide steps for deployers to adhere to privacy principles regarding consent, use limitation, storage, and accountability

BioPrivacy *Application Evaluation*

- *Central privacy considerations in biometric applications*
 - Overt vs. Covert
 - Opt-in vs. Mandatory
 - Verification vs. Identification
 - Fixed Duration vs. Indefinite Duration
 - Private Sector vs. Public Sector
 - Individual / Customer vs. Employee / Citizen
 - User Ownership vs. Institutional Ownership
 - Personal Storage vs. Template Database
 - Behavioral vs. Physiological
 - Templates vs. Identifiable Data
- Primary applications: physical access, network security, civil ID, retail/point of sale

BioPrivacy *Technology Risk Ratings*

- *Central privacy considerations in biometric technologies*
 - Verification/Identification
 - Overt/Covert
 - Behavioral/Physiological
 - Interoperable/Closed
- As technologies improve & markets change, potential privacy invasiveness of technologies can also change

Technology Risk Rating: Higher

- Facial recognition

- Verification/ identification: H
- Behavioral/physiological: M
- Overt/covert: H
- Interoperable/closed: H
- Overall Risk Rating: H

- Fingerprint

- Verification/ identification: H
- Behavioral/physiological: H
- Overt/covert: L
- Interoperable/closed: H
- Overall Risk Rating: H

Technology Risk Rating: Medium

- Iris recognition
 - Verification/ identification: H
 - Behavioral/physiological: H
 - Overt/covert: L
 - Interoperable/closed: M
 - Overall Risk Rating: M

Technology Risk Rating: Lower

- Hand geometry
 - Verification/ identification: L
 - Behavioral/physiological: M
 - Overt/covert: L
 - Interoperable/closed: M
 - Overall Risk Rating: L
- Signature
 - Verification/ identification: L
 - Behavioral/physiological: L
 - Overt/covert: L
 - Interoperable/closed: L
 - Overall Risk Rating: L
- Speaker verification
 - Verification/ identification: L
 - Behavioral/physiological: L
 - Overt/covert: M
 - Interoperable/closed: L
 - Overall Risk Rating: L

BioPrivacy *Best Practices*

- Recommendation: implement as many Best Practices as possible without undermining core system operations
- Few if any applications will be able to adhere to all BioPrivacy Best Practices
 - Inability to comply with certain Best Practices is balanced by adherence to others
- Four Categories
 - Scope and Capabilities
 - Data Protection
 - User Control Of Personal Data
 - Disclosure, Auditing and Accountability

Scope and Capabilities

- Limit system scope
 - Even slight expansions of scope should be limited
- Limit retention of biometric information
 - While enrollment data is stored in most systems, verification data can usually be discarded
- Limit storage of identifiable biometric data
 - Actual images, recordings, and identifiable biometric data should be discarded when possible
- Limit collection, storage of extraneous information
 - Collect non-biometric data only as necessary
- Make provisions for system termination
 - Establish a policy to de-populate, dismantle system

Data Protection

- Use security tools to protect biometric information
 - Encryption, private networks, and secure facilities to protect biometric information at all stages of lifecycle
- Protect post-match decisions
 - “Match”, “non-match” and “error” data transmissions need to be protected
- Limit system access
 - Prevent internal compromise by limiting access to biometric data to small group of system operators

User Control Of Personal Data

- Make system usage voluntary and allow for “un-enrollment”
 - Allow users to opt-out after enrollment
- Provide means of correcting and accessing biometric-related information
 - Allow users to view, correct and update information stored in biometric system
 - Allow users to re-enroll if necessary

Disclosure, Auditing, Accountability

- **Disclose system purpose and objectives**
 - Explain purpose of system to operators, enrollees
 - Disclose whether enrollment is opt-in or mandatory
 - Disclose fallback procedure
- **Hold operators accountable for system misuse**
 - Disclose who is responsible for system
 - Provide a means of dispute resolution
- **Disclose use of system**
 - When enrollment or verification is taking place
- **Make provisions for third-party auditing, oversight**
 - Operational oversight and review critical to all systems

Changing System Design Assumptions

- Biometric system design assumptions relevant to privacy have changed in many emerging applications
 - US-VISIT, registered traveler, employee access control
- Interoperability
 - Then: interoperability poses privacy risks
 - Now: interoperability a critical requirement
- Data formats
 - Then: biometric systems should store only encoded templates
 - Now: biometric systems retain images for future-proofing
- Data capture
 - Then: always informed consent for data capture
 - Now: substantial advanced research in covert capture

Areas for Consideration

- Where is privacy prioritized relative to factors such as cross-jurisdictional interoperability, long-term utility?
- How will disputes over biometric data collection for border management be resolved?
- In what applications is opt-out viable?
- How does biometric systems' ability to deal with “fake” biometrics impact the discussion?
- What is the threshold for identity certainty in biometric systems?