

# 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

## Identifying and Reducing Privacy Risks in Biometric Systems

---

**13th Annual Conference on Computers, Freedom & Privacy**  
**The New Yorker Hotel, New York City – 4 April 2003**  
**Michael Thieme, Director of Special Projects**  
**[mthieme@biometricgroup.com](mailto:mthieme@biometricgroup.com)**

# Agenda

---

- Defining the Problem
- Evaluating Risks through the BioPrivacy Framework
- Current Trends and Developments

# About International Biometric Group

---

- Independent biometric research, consulting and technology solutions firm, founded in 1996
  - Offices in New York and Washington, D.C.
- Technology-neutral and vendor-independent
  - Extensive experience across all biometric technologies
  - IBG does not resell or distribute biometric hardware
- Advises government and corporate clients in effective use of biometrics
  - Will the technology address program requirements?
  - What are the risks and costs?
  - What technologies are likely to work effectively?
  - What are the privacy risks?

# IBG Privacy Background and Experience

---

- Developed *BioPrivacy Initiative*, an evaluation framework that establishes criteria for evaluating the potential privacy impact of biometric deployments, technologies
- Advocates detailed Best Practices to ensure that biometrics are deployed in a privacy-protective and/or privacy-sympathetic fashion
- Conducted privacy-related biometric assessment work for Transportation Security Administration, California DMV, White House OSTP, Hong Kong Immigration Department

---

# Defining the Problem

# Basic Questions

---

Are biometric templates personal information?

Under what circumstances is  
biometric usage privacy invasive?

Which technologies pose the most serious threats,  
and why?

# Biometric Privacy Concerns

---

- Personal Privacy
  - Inherent discomfort with or opposition to biometrics
  - Perception of invasiveness
  - *No means of logically addressing these concerns*
- Informational Privacy
  - Function creep
  - Use as unique identifier
  - Associating unrelated data
  - Use by law enforcement agencies without oversight
  - Concerns generally predicated on misuse of technology as opposed to intended uses
  - *Some portion of these concerns can be addressed through technology, best practices, deterrents to misuse*

# When Is Biometric Data “Personal” Data?

---

- Personal Data...
  - *Data which relate to a living individual who can be identified –*
    - *from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller...*
- [www.n-i.nhs.uk/dataprotect/guidance/Index/guidance/legal/personal\\_data\\_definition.htm](http://www.n-i.nhs.uk/dataprotect/guidance/Index/guidance/legal/personal_data_definition.htm)
- Compare to a position held by a biometric industry group...
    - *“Biometric data is electronic code that is separate and distinct from personal information.” – IBIA*
  - In a very narrow sense, *certain* biometric data can be seen as separate and distinct from personal information
    - *However, when biometric data itself is the object of collection and interest, then it should be viewed as personal data*

# Why Do Biometric Templates Matter?

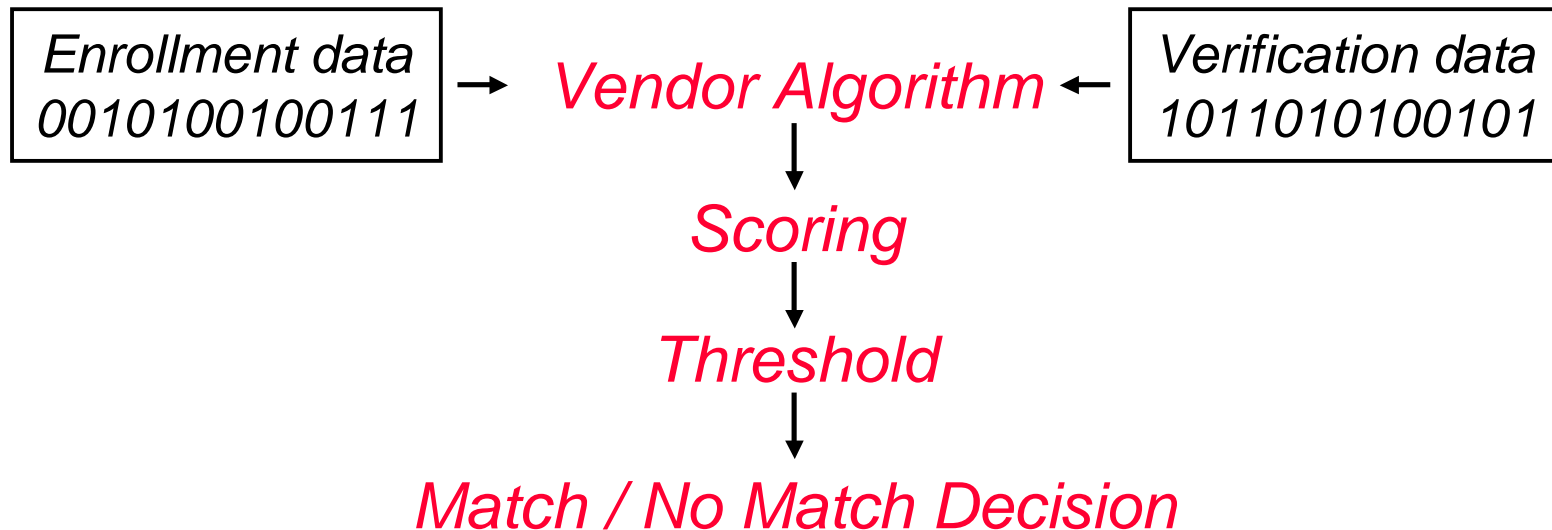
---

- Biometric Templates: distinctive, encoded files derived from the unique features of a biometric sample
  - Created during enrollment and verification/identification
- A basic building block of biometric systems, central to understanding real privacy issues
  - Templates, not images/samples, are used in biometric matching
  - Much smaller amount of data than sample (1/100th, 1/1000th)
  - Some, not all, systems retain images for manual inspection, open interoperability
- Not normally possible to reverse-engineer sample from template
  - Although this is not an absolute truth – very simplistic systems can be attacked in this fashion
- *Vendor templates are not interchangeable and cannot realistically be compared or tracked against each other; the data formats are not compatible*

# Why Does The Matching Process Matter?

---

- Comparing strings of binary data (templates)
- Result of match (“score”) compared to pre-determined threshold – system indicates “match” or “no match”
- Biometric systems do not provide a 100% match – only a probability
  - Why? Templates (even from the same fingerprint) are highly variable, and are not identical
  - A 100% match means that your system has been compromised



# Are Biometrics Unique Identifiers?

---

- Yes, because...
  - A piece of biometric data can be tied to an individual with a high degree of certainty
  - Many biometrics characteristics are effectively “unique” to the person (e.g. fingerprints, irises)
- No, because...
  - Biometric data changes over time (even from minute to minute), therefore biometrics alone cannot function as unique, stable keys
  - Most biometrics cannot be tracked across disparate databases, particularly when in template form, and therefore cannot function as unique identifiers (as opposed to ID numbers)
- The argument “you only have one thumb” not compelling
  - Millions of enrollment templates can be generated for each thumb
  - Well-designed systems can survive the compromise of biometric data
- *The answer depends on your definition of uniqueness*

# How Is Biometric Accuracy Measured?

---

- System accuracy defined through three metrics
  - False match (*imposter breaks in*)
  - False non-match (*correct user locked out*)
  - Failure to enroll (*user cannot register in system*)
- Vendor claims (1/1000, 1/1000000) are not always based on experience in real-world deployments
- Comparative testing shows that some devices and technologies provide very high accuracy, others very low accuracy
- Regardless of technology, some small percentage will be unable to enroll
- *Biometrics are NEVER perfect*

---

# Evaluating Real Privacy Risks through the BioPrivacy Framework

# Protective, Sympathetic, Neutral, Invasive

## Privacy-Invasive

Systems capture biometrics without knowledge or consent; biometric used for undisclosed purposes or beyond initial scope  
*(certain national ID, surveillance)*

## Privacy-Neutral

Use of biometrics does not bear any strong relation to privacy  
*(personal PDA, home PC, access control)*

## Privacy-Sympathetic

Systems with specific design elements to ensure biometric data is protected from unauthorized access and usage  
*(most apps can incorporate privacy-sympathetic elements)*

## Privacy-Protective

Systems use biometrics to protect personal information which might otherwise be compromised  
*(enterprise security, accountholder verification)*

# IBG's BioPrivacy Initiative

---

- Analysis Of Biometric Applications
  - **BioPrivacy Impact Framework**: not all biometric deployments bear the same privacy risks: specific features of biometric deployments increase or decrease the likelihood of misuse
- Analysis Of Core Biometric Technologies
  - **BioPrivacy Technology Risk Ratings**: certain technologies are more prone to be misused than others and require extra precautions
- Steps Towards A Privacy-sympathetic System
  - **BioPrivacy Best Practices**: ensure that deployers adhere to privacy principles regarding consent, use limitation, storage limitation, and accountability

# Applications: BioPrivacy Impact Framework

---

- Q: What are the fundamental characteristic of a biometric application central to its privacy impact?
- **Impact Framework** defines ten factors critical to identifying potential privacy risks within a biometric application
- Why this matters
  - **Blanket statements about biometrics without understanding the technology's application are misleading**
  - If all biometric applications are clustered under one risk rating, objections to truly invasive biometric systems will be crying wolf
  - Among deployers, privacy is not an absolute, and risks are weighed and evaluated against benefits

# BioPrivacy Impact Framework Criteria 1-5

---

## 1. Overt vs. Covert

- Covert deployments (surveillance without signage) are by definition more likely to be privacy invasive

## 2. Opt-in vs. Mandatory

- Opt-in deployments are much less likely to receive privacy-related scrutiny than mandatory deployments

## 3. Verification vs. Identification

- If the core technology is capable of searching databases of biometric records, there is greater potential for misuse
- Many biometrics simply *cannot be searched*

## 4. Fixed Duration vs. Indefinite Duration

- Certain deployments can be terminated after a certain period of time, reducing privacy risks

## 5. Private Sector vs. Public Sector

- This may be debatable, but public sector deployments are more susceptible to privacy invasive uses due to law enforcement interests, less fear over public outcry

# BioPrivacy Impact Framework Criteria 6-10

---

## 6. Individual / Customer vs. Employee / Citizen

- The individual's role is central to privacy impact – the risks apply roughly in this order (Individual, customer, employee, citizen)

## 7. User Ownership vs. Institutional Ownership

- If the user retains usage rights over the data, the risks are much lower

## 8. Personal Storage vs. Template Database

- If the user is in possession of the biometric data, risks are fewer
- Many systems are being designed with both central and local storage in mind

## 9. Behavioral vs. Physiological

- Physiological data (fingerprint, iris) is more likely to be used in an invasive fashion than behavioral data (voice)

## 10. Templates vs. Identifiable Data

- Templates are less likely to be utilized in a privacy-invasive fashion than images/samples

# Technology: BioPrivacy Risk Ratings

---

- Some technologies have almost no privacy impact, and cannot realistically be used in a privacy-invasive fashion
- Others are much more susceptible to privacy-invasive usage, due to core operation or extrinsic factors
- Four factors used to rank a technology's potential privacy risk (**Low, Medium, High**)

## 1. Verification / Identification

- Is the core technology capable of searching databases of biometric records?

## 2. Overt / Covert

- Can the biometric technology be used in a covert fashion?

## 3. Behavioral / Physiological

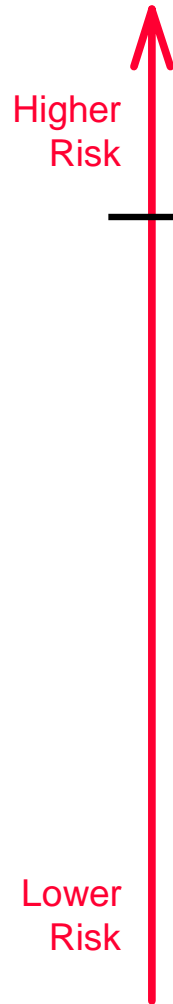
- Is the biometric based on behavioral or on physiological traits?

## 4. Compatible with Existing Databases

- Are there currently databases against which this biometric can be searched?

# Technology Risk Rating: High

---



- Facial Recognition

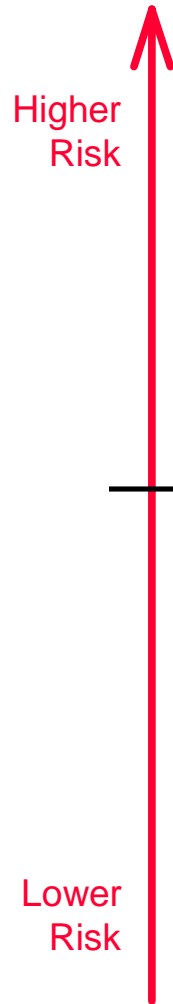
- Verification / Identification: H
- Behavioral / Physiological: M
- Overt / Covert: H
- Database Compatibility: H
- Overall Risk Rating: H

- Fingerprint

- Verification / Identification: H
- Behavioral / Physiological: H
- Overt / Covert: L
- Database Compatibility: H
- Overall Risk Rating: H

# Technology Risk Rating: Medium

---



- Retina-scan

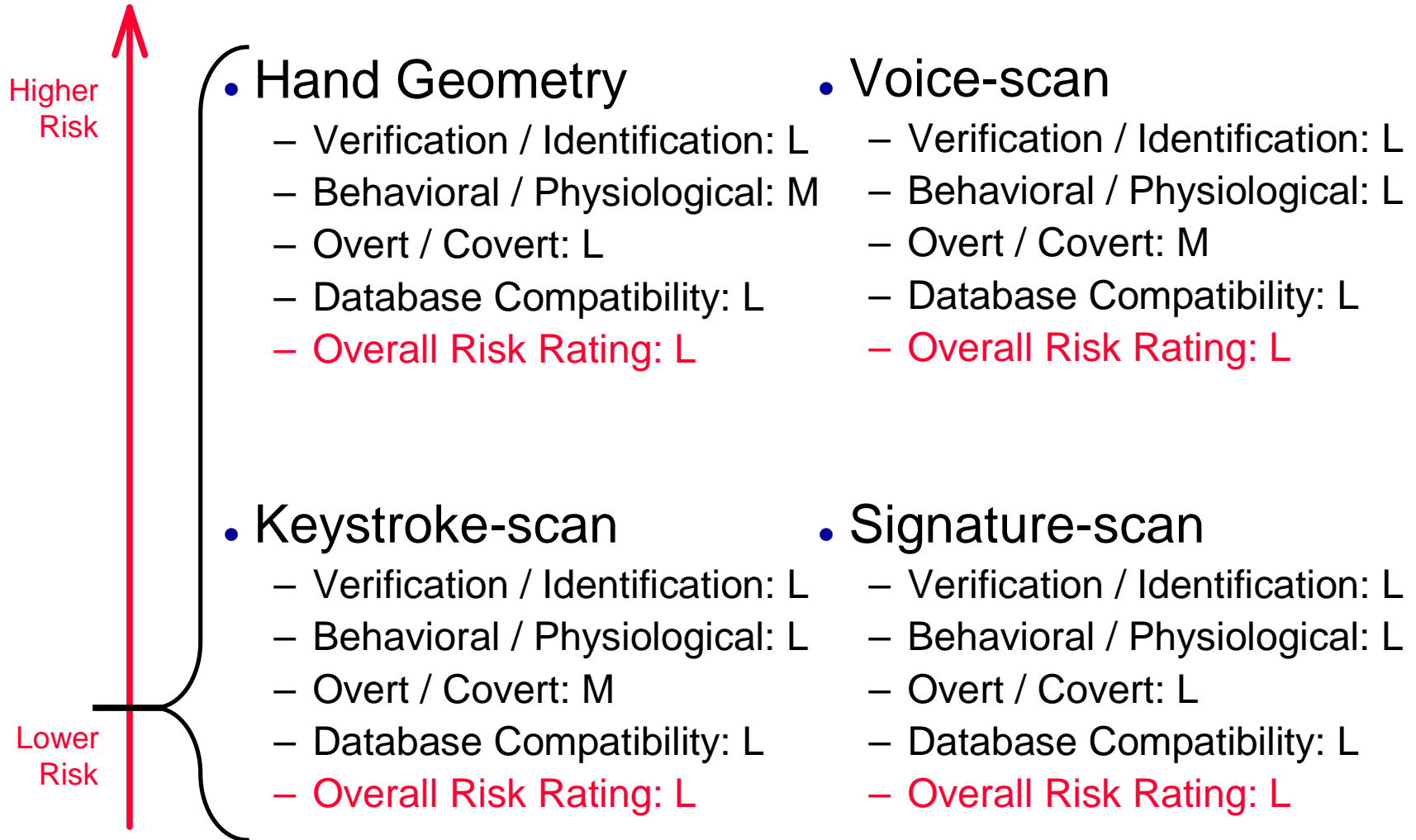
- Verification / Identification: H
- Behavioral / Physiological: H
- Overt / Covert: L
- Database Compatibility: L
- Overall Risk Rating: M

- Iris-scan

- Verification/ Identification: H
- Behavioral / Physiological: H
- Overt / Covert: L
- Database compatibility: L
- Overall Risk Rating: M

# Technology Risk Rating: Low

---



# BioPrivacy Best Practices

---

- Guidelines for privacy-sympathetic and privacy-protective deployment
- Provides institutions with an understanding of the types of protections and limitations commonly implemented
- Few if any applications will be able to adhere to all BioPrivacy Best Practices
  - *Implement as many Best Practices as possible without undermining the basic operations of the biometric system*
  - Inability to comply with certain Best Practices is balanced by adherence to others

# Categories of BioPrivacy Best Practices

---

- 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

---

# Current Trends and Developments

# Trends / Developments: Border Entry

---

- U.S. Legislation mandates that certain alien passports and visas utilize biometrics by 10/2004
  - Equipment must also be deployed to read such documents
- For passports...
  - International Civil Aviation Organization will likely recommend biometric facial recognition, contactless chip card
- For visas issued through U.S. consulates...
  - National Institute of Standards and Technology leaning toward combination of 2 fingerprints and facial image
- Both are image-based, not template-based, standards
- Potential privacy impact
  - *May have implications for U.S. passports, ID documents (which are not addressed under this legislation)*

# Trends / Developments: Employee Cards

---

- U.S. transportation workers to eventually be issued standardized ID card (TWIC) that utilizes biometrics
  - Designed to secure access to controlled areas
  - Which biometric or combination of biometrics?
  - What type of card?
  - What data format?
- DoD currently issuing Common Access Cards, some will use biometrics
- Potential privacy impact
  - *Cards may come to be used for broader purposes*

# Trends / Developments: Qantas Airways

---

- Proposed 600-person deployment for Time and Attendance to combat buddy-punching
- Union threatened strike if system implemented
  - Seen as privacy-invasive, a potential tool to “track” employees, in violation of enterprise bargaining agreement...
- System withdrawn
- Potential privacy impact
  - *May signal increased resistance to technologies which, correctly or incorrectly, are viewed as “tracking” technologies*

# Trends / Developments: Spoofing

---

- We have learned through simple tests that many biometric systems can be defeated through fake fingers
  - Finger, face, voice, iris, hand...
  - Some easily broken, others took time
- Does this help or hurt privacy?
- This helps privacy because...
  - It underscores the fact that a biometric match is one of many considerations in identity determination: it is not the last word
- This hurts privacy because...
  - Individuals may have their information accessed or compromised through the use of such “spoofs”
- *Spoofing is a non-issue in many usage environments, a real issue in others*

# Observations

---

- Few in the biometric industry have an understanding of, or concern for, privacy principles
  - Many of those with an awareness of privacy view it as a technology problem
- Few privacy experts have a sufficient understanding of biometrics to fully understand actual vs. nonexistent risks
  - Credibility can be undermined when outlining scenarios incompatible with basic operations of technology
- *In what situations is energy best spent in fighting against biometric deployment versus ensuring that such usage is compliant with general privacy principles?*

# Thank You

---

Michael Thieme  
International Biometric Group  
212-809-9491  
mthieme@biometricgroup.com