Privacy Implications of Iris Technology

Walter Hamilton
Vice Chairman
International Biometrics + Identity Association

IBIA Identity Matters

IBIA's Mission

The International Biometrics + Identity Association (IBIA) is a non-profit trade association that advances the adoption and responsible use of technology-based identification solutions to manage identity and to enhance security, privacy, productivity, and convenience. This mission applies to government, business, and consumer uses.

Biometrics and Privacy

- All technology – including biometrics – is inherently privacy neutral
  - It is the application that determines whether a technology is privacy enhancing or a privacy threat
- Privacy concerns are legitimate and can delay adoption of biometrics if not adequately considered and addressed
- Iris technology shares most of the same privacy risks as other biometric modalities
  - Iris pattern is not a secret
  - Is visible to others
  - Is permanent and not easily revocable
  - An enrollment or recognition template created for one purpose could be misappropriated and used for fraudulent purposes

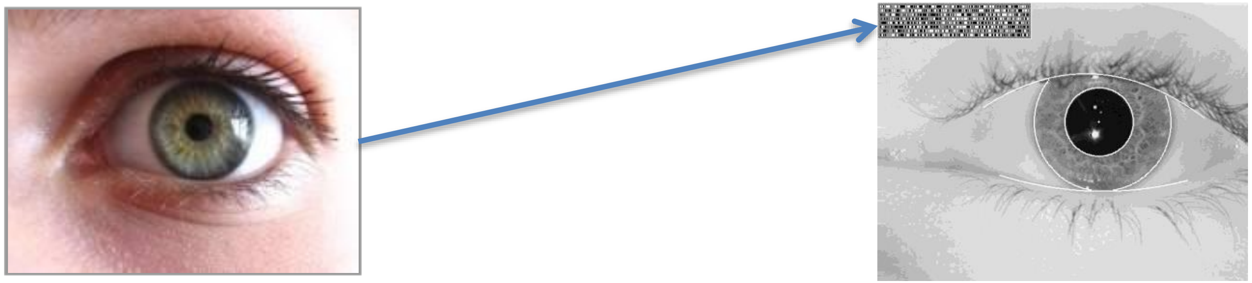
Biometric Privacy in the U.S.

- There is no uniform legal framework regarding biometric privacy in the U.S.
- In Europe, by law, any information that can point to a given individual SHALL be under the control of the individual
- Generally, biometric data should be considered as personally identifiable Information (PII) and treated accordingly
- Primary concern is theft of biometric data or sensor spoofing to obtain unauthorized access or privileges
- Other concerns are presented by organizations that acquire large biometric databases where there is no notice, consent, opt in/out or where there is unauthorized data sharing

Iris Considerations

- Can be acquired passively from a distance of up to 40 feet
  - Iris-in-a-crowd surveillance is not practical yet, but….
- Primary application is physical access or logical access control
  - Becoming a biometric modality in intelligence/military/law enforcement databases
- Now being integrated into consumer smart phones
- Could become significant factor in mobile payments/transaction authorization

Iris Template Generation



- No need to store iris image for access control applications
- Template has less utility for sensor presentation attack scenarios
- Restrict access if image is retained for purposes of interoperability or algorithm refresh without re-enrollment

Prevent Unauthorized Use of Iris Data

- Recognize/address the possibility of leakage or theft of iris data
- Retain iris data only in template form if possible
- Encrypt biometric data when stored or in transit
- Store and match on device or in secure element
- Secure channel between sensor and any external components
- Digitally sign biometric data
  - Prevent unauthorized alteration or replacement of data
- Flag data type as enrollment or matching to prevent playback attacks
- Consider revocable biometric template transformation
  - Application/transaction-specific templates

Presentation Attack Scenarios

- Use a photograph of the target iris pattern
- Painted iris pattern contact lenses

Preventing a Presentation Attack

- Since irises can be scanned passively, it is possible to acquire and present a fake iris to an iris sensor and gain access
- Some iris sensors/systems now include presentation attack detection (PAD)
  - But there is no authoritative data on the robustness of these techniques
- NIST has proposed that a biometric system used for government digital authentication SHALL demonstrate at least 90% resistance to presentation attacks[1]
  - But there is no accredited independent laboratory that provides such validation services for the vendor community
  - Normative technical requirements should be "testable"

[1] *NIST Special Publication 800-63B – Digital Authentication Guideline (DRAFT)*

IBIA Perspective

- There are legitimate concerns over the potential misuse of biometric data
- Biometric data should be protected as appropriate for any other personally identifiable information
- Implementers should develop policies that clearly set forth how biometric data will be collected, stored, accessed and used
  - Limit distribution of biometric data for any reason beyond the stated purposes
  - Establish security requirements for binding between biometric data and an identity reference
  - Analyze threats and develop countermeasures

Final Thoughts

- Consider the attacker's degree of difficulty (time, effort and cost) vs. the value of the target
  - How easy is it to exploit vs. other non-biometric hacks
  - Consider multi-modal or multi-factor authentication if target value is high
- Consider the risk to the attacker
  - Chance of apprehension when direct physical presence at the sensor is required for a presentation attack
- Consider the potential harm to the individual whose biometric data is compromised
- Develop appropriate policies and procedures to protect privacy

IBIA

International
Biometrics+Identity
Association

For more information please visit
our website: **ibia.org**