TECHNICAL PRIVACY SAFEGUARDS FOR FACIAL RECOGNITION

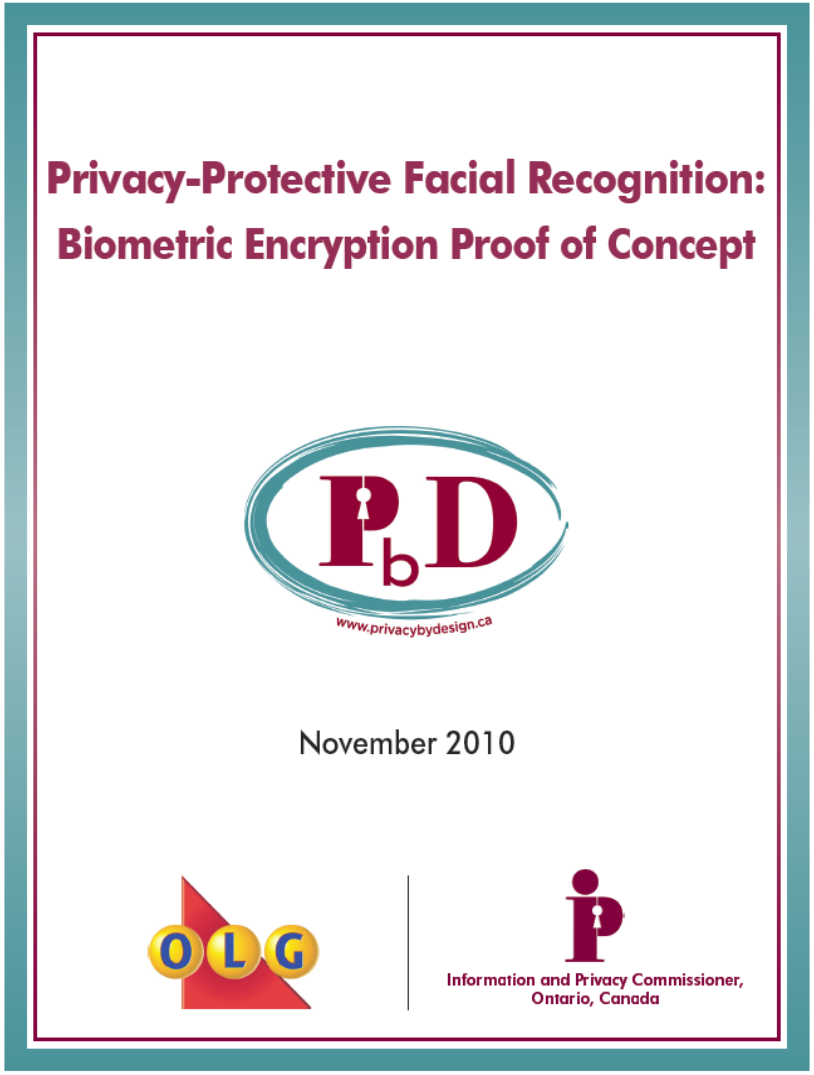
Panel 3
US Department of Commerce
NTIA – Privacy Multi-stakeholder Meeting
Washington, D.C.

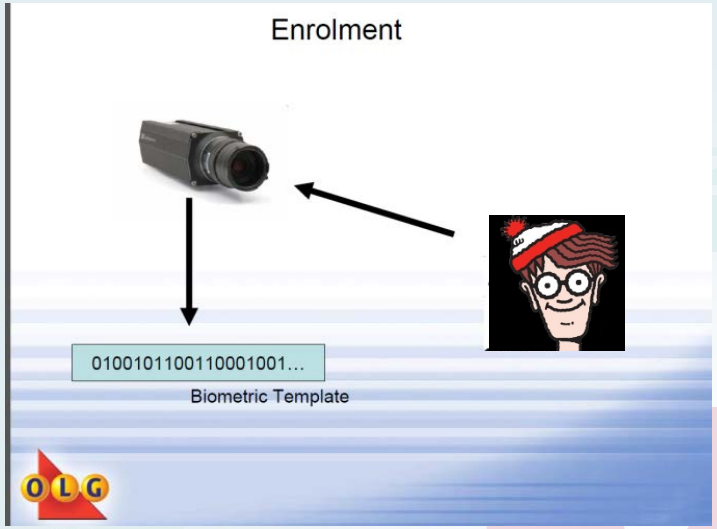
February 6, 2014

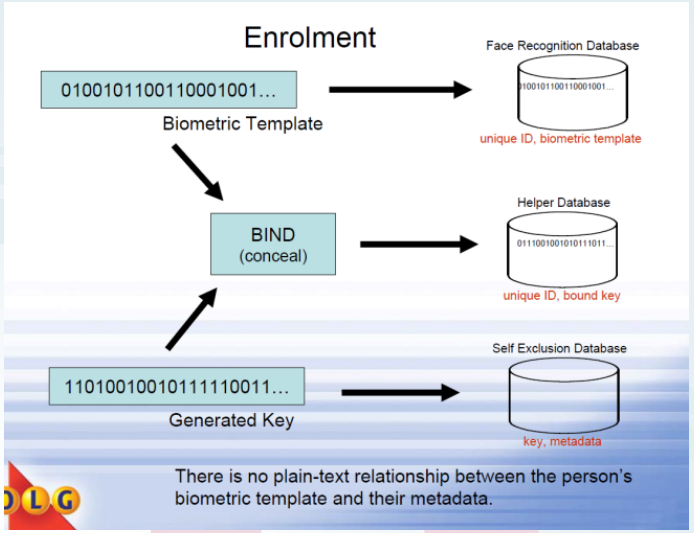
Information and Privacy Commissioner of Ontario

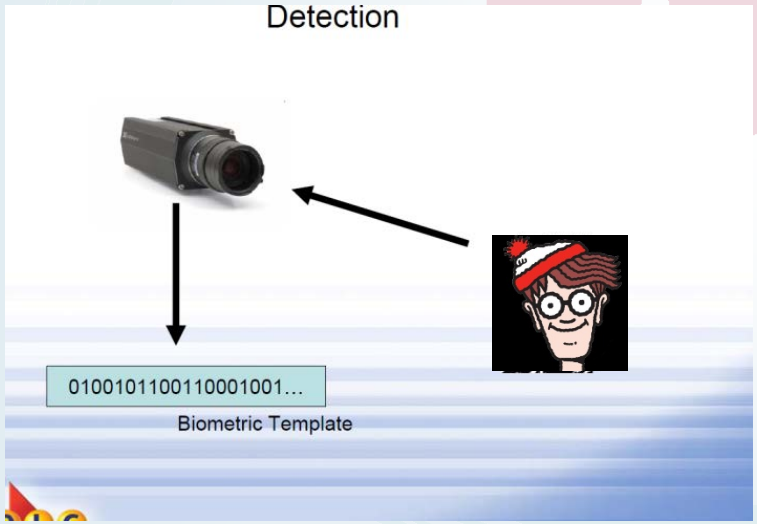
Facial Recognition + Biometric Encryption: Proof of Concept

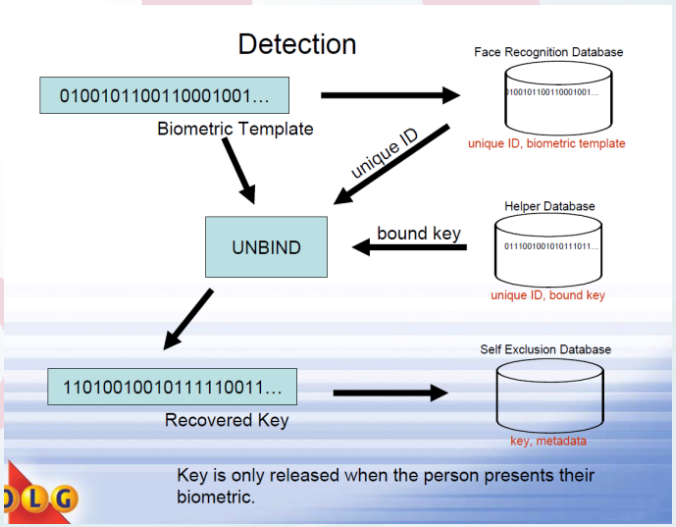
- Live field test at casino: Correct Identification Rate (CIR) is 91% without BE, and 90% with BE – negligible accuracy impact
- BE reduces False Acceptance Rate (FAR) by up to 50% – a huge improvement in accuracy
- Accuracy exceeds state-of-the-art for facial recognition
- Triple-win: privacy, security, and accuracy (unexpected) – all improved











If unbind is unsuccessful – i.e. person is not on the self-exclusion list, all captured information is discarded.

Source: IPC/PbD November 2010

Remote authentication using FR-BE in Match on Card architecture

Fresh FR template

Match-On-Card

Templates match

Regenerate Biometric key, BK'

Stored FR template

Challenge - response

OK

BK = BK'

Remote verifier

Stored BK

J.Bringer and H.Chabanne, 2008; 2013

Advantages of the FR-BE MOC system

- Two integrated pieces of authentication (“what you have” and “who you are”)
- Resilient against the substitution attack since the Biometric Key (BK) is generated from the user’s biometric;
- Coding, storage, and the matching are performed on the card under the control of the user;
- Smartcard is tamper resistant;
- The smartcard cannot be loaned to another user;
- The server stores BK that is generated from biometric but cannot be reverse engineered;
- The server’s database cannot be linked with other biometric databases;
- It even cannot be linked with other databases that store BKs since a BK generated for the same user but from a different capture will be completely different;
- The accuracy of the state-of-the-art facial recognition is preserved;
- The overall system is a triple-win for security, privacy, and accuracy – all the trademarks of the Privacy by Design approach.

Privacy Visor glasses Justice Caps

Privacy visor glasses – cont'd

- Developed by Japan's National Institute of Informatics
- Light from these near-infrared Light Emitting Diodes (LEDs) can't be seen by the human eye, but when it passes through a camera's imaging device, it appears bright
- Both face detection and face recognition fail
- Sunglasses may not be enough anymore
- Earlier product: "Justice caps", already available

Privacy Preserving Video Surveillance System

- Video surveillance is here to stay
- Video surveillance must have built-in privacy protecting capabilities: Privacy by Design
- K. Martin and K. N. Plataniotis, 2008
- F. Qureshi, 2006 - 2013

Innovative Privacy-Enhancing Video Surveillance

- This technology uses cryptographic techniques to secure a private object so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key;
- Objects of interest (face or body) are stored as completely separate entities from the background surveillance frame, and efficiently encrypted.

(a) (b) (c)

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

Source: IPC Privacy Investigation Report Privacy and Video Surveillance in Mass Transit Systems, March 2008.

Privacy Preserving Video Surveillance Prototype (Under Development at UOIT)

Object Video Streams

Encrypted Video Transmission Channel

Encrypted Storage

Online Monitoring

Video Analytics

Video Encryption

Object Centric Monitoring

How to Contact Us

Michelle Chibba, Director, Policy and Special Projects
Information and Privacy Commissioner's Office of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073
Web: www.ipc.on.ca / www.privacybydesign.ca
E-mail: info@ipc.on.ca