Excuse Me: Is This You?

Ken Anderson

Assistant Commissioner (Privacy)

Ontario

Canada Conference Board Council of Chief Privacy Officers

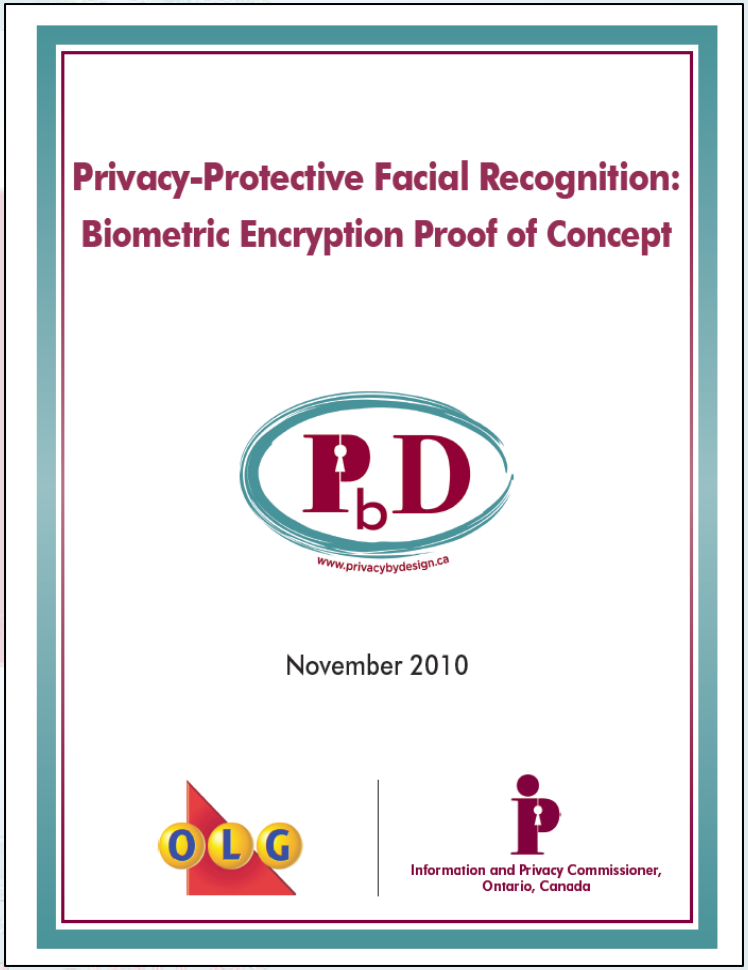
January 25, 2011

Presentation Outline

1. *Biometric Facial Recognition*
2. *Biometric Encryption*
3. *Questions and Answers*

Biometric Encryption:
The Privacy by Design Approach

"The rapid, accurate identification and authentication of individuals has become a challenge across many sectors and jurisdictions … Increasingly, biometric encryption is being viewed as the ultimate means of authentication or identification across a broad range of applications."



OLG Facial Recognition Program

- The system is designed to detect only self-excluded people – not cheaters or organized crime;
- Legacy, photograph-based system, needs to be maintained without the need for re-enrolment of individuals;
- Automated facial recognition system is the only technology that produces remote identification and is compatible with the legacy photograph-based system.

OLG Facial Recognition Program

- OLG is subject to Ontario's privacy legislation;
- To their credit, OLG contacted us at the earliest stage and adopted the Privacy-by-Design approach – embedding the privacy protection means directly into the core technology;
- The research project was successfully completed at the University of Toronto, developing an essentially new variant of a BE algorithm called Quantized Index Modulation (QIM);
- The database tests showed that BE may be integrated with conventional facial recognition, with little or no accuracy degradation.

OLG Self-Exclusion program

- Completely voluntary self-excluded individuals – more than 12,000 in Ontario and growing;
- **Great Need** for reliable detection of those attempting to enter a gaming site – manual comparison alone does not work;
- Privacy of all casino patrons must be protected;
- **Solution:** Facial recognition in watch-list scenario with the use of *Biometric Encryption*;
- Novel ***"Made in Ontario"*** PbD application: collaboration of OLG, IPC, UofT, and iView Systems.

Facial Recognition with Biometric Encryption

- ***Biometric Encryption*** (BE): securely binds a person's identifier (pointer to personal information) with facial biometrics;
- The pointer is retrieved only if a correct (i.e., self-excluded) person is present;
- The link between facial templates and personal information is controlled by BE;
- Final comparison is done manually;
- Privacy of both the general public ***and*** self-excluded individuals is protected.

Proof of Concept

- Live field test at Woodbine facilities: 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;
- **Next:** production version of facial recognition with BE.

Biometric Encryption (BE)

What is Biometric Encryption?

- Class of emerging “untraceable biometrics” technologies that seek to translate the biometric data provided by the user;
- Special properties:
  - uniqueness
  - irreversibility

Possible Applications and Uses of Biometric Encryption

- Biometric ticketing for events;
- Biometric boarding cards for air travel;
- Identification, credit and loyalty card systems;
- “Anonymous” labeling of sensitive records and files (medical, financial);
- Consumer biometric payment systems;
- Access control to personal computing devices;
- Personal encryption products;
- Local or remote authentication to access files held by government and other various organizations.

Privacy Benefits of Biometric Encryption

- A unique biometric template does not exist;
- Code breaking now a security issue not a privacy issue;
- Can have as many PINs as separate applications;
- Security can be enhanced with challenge-response systems;
- Can evolve toward a cardless society.

Advantages of Biometric Encryption

BE Embodies core privacy practices:

1. Data minimization: no retention of biometric image or template, minimizing potential for unauthorized secondary uses, loss, or misuse;
2. Maximal individual control: Individuals may keep their biometric data private, and can use it to generate or change unique ("anonymous") account identifiers, and encrypt own data;
3. Improved security: authentication, communication and data security are enhanced.

Discussion

Q's & A's

How to Contact Us

Ken Anderson
Assistant Commissioner (Privacy)

IPC 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

E-mail: info@ipc.on.ca