

Privacy by Design Curriculum 2.0

Instructor Resources

MODULE TWO: APPLIED PRIVACY BY DESIGN

Presentation 5: *Biometric Encryption*



CONTENTS

Overview	2
Essential Reading	2
Learning Objectives	2
<i>Biometric Encryption: Overview of Presentation</i>	3
Further Reading	4
Presentation Materials with Instructor Notes	5



Overview

This section outlines the growing need for identification and authentication in the online and off-line worlds, and highlights the various forces that are undermining traditional, trust-based models.

It suggests a possible role for biometrics – using physical or physiological characteristics to recognize, authenticate, and/or verify identity – but identifies significant privacy and operational concerns with traditional biometrics. It then goes on to demonstrate how the application of the 7 Foundational Principles of *Privacy by Design* to biometrics, as reflected in Biometric Encryption, is the embodiment of *PbD* and the delivery of both privacy and security. It concludes with an example of how privacy-protective facial recognition is being applied by the Ontario Lottery and Gaming Corporation in its gaming facilities.

Essential Reading

A. Cavoukian and A. Stoianov, [Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. www.ipc.on.ca](http://www.ipc.on.ca)

Information and Privacy Commissioner, Ontario and Ontario Lottery and Gaming Corporation, [Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept. www.ipc.on.ca](http://www.ipc.on.ca)

Dr. Ann Cavoukian, Information and Privacy Commissioner/ Ontario, and Dr. Alex Stoianov, [Biometric Encryption Chapter from the Springer Encyclopedia of Biometrics. www.ipc.on.ca](http://www.ipc.on.ca)

Learning Objectives

Participants will develop an understanding of identification and authentication requirements in the online and off-line worlds, and an appreciation of the significant risks that are associated with using traditional biometrics to meet these requirements.

They will become familiar with the concept of biometric encryption, and explore how it has been applied in a real-world scenario to deliver both privacy and security in a win-win, positive sum outcome.

Biometric Encryption: Overview of Presentation

Slide	Title	Theme
5.1	The Context	Identification and authentication requirements are steadily increasing
5.2	Challenges to the Trust Model	Current technology and practice is putting trust under pressure
5.3	Alternatives to Trust	Emerging roles for biometrics
5.4	Biometrics: A Primer	Biometrics is a two-stage process
5.5	Privacy and Security Issues in Biometric Systems	Biometrics raise significant privacy issues, particularly when used for identification (as opposed to authentication)
5.6	Traditional Biometrics: A Dead End for Privacy	Privacy issues are so significant that biometrics have been a dead end
5.7	Traditional Biometrics: The Bottom Line	Traditional biometrics force a choice between privacy or security
5.8	<i>Privacy by Design</i>	The principles of PbD offer an alternative instead of a choice
5.9	Biometric Encryption	Privacy and security (not versus)
5.1	Biometric Encryption: Process Overview	A description of how the process works
5.11	Advantages of BE over Traditional Biometrics	BE addresses many of the concerns associated with traditional biometrics
5.12	From Theory to Practice: The Ontario Lottery and Gaming Corporation (OLG) Self Exclusion Program	Application of BE in Ontario, Canada casinos and gaming sites
5.13	Privacy- Protective Facial Recognition	White paper on privacy-protective facial recognition
5.14	Sample Application of BE	Process flow for privacy-protective facial recognition technology
5.15	Facial Recognition using BE	Key features of the OLG application
5.16	Lessons Learned: Benefits of Applying <i>PbD</i>	Fosters innovation, meets all requirements, improves functioning of the system, both privacy and security

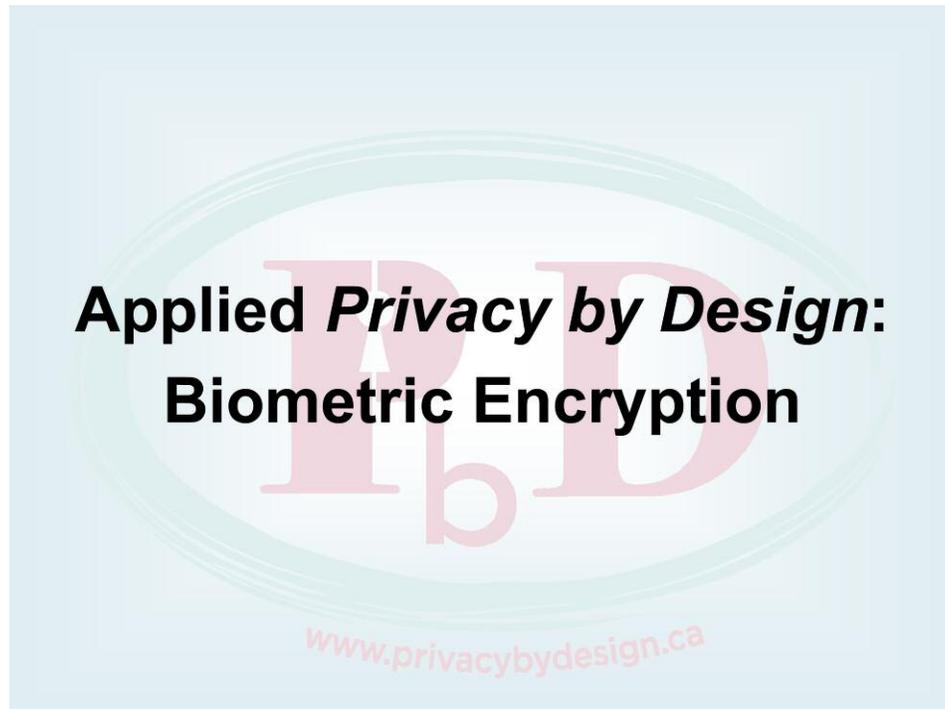
Further Reading

Ann Cavoukian, Ph.D, Information & Privacy Commissioner, Ontario and Max Snijder, CEO, European Biometrics Forum and Chairman of the International Biometrics Advisory Council (IBAC), [The Relevance of Untraceable Biometrics and Biometric Encryption: A Discussion of Biometrics for Authentication Purposes](#). www.ipc.on.ca

Information & Privacy Commissioner, Ontario, [Z Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age](#). www.ipc.on.ca

National Science & Technology Council Subcommittee on Biometrics and Identity Management. [Biometrics History](#). <http://www.biometrics.gov/Documents/BioHistory.pdf>

Presentation Materials with Instructor Notes



Slide 1

The Context

Growing need for online *and* offline
identification and authentication

Accounts...Physical Access...Memberships
Online shopping...System Access...
Networks...Gaming...Forums...

Built on **TRUST**

www.privacybydesign.ca

Slide 2

Identification and authentication requirements are steadily increasing in both the online and offline worlds.

There is a great need on the part of both public and private sector entities to “know” who they are dealing with. Currently, the typical security model is based on using a token, which represents an individual, to either authenticate identity or allow access to information, premises or services. This token may be:

- a password or shared secret [something you know],
- an identity card (something you have), or
- a biometric (something you are).

In all of these cases, the details of the token are held by a person or system whose function is to evaluate and authorize transactions where the details of an individual’s token match those stored in a database or record.

Traditionally, the relationship between the individual who provides the information and organization that receives it is largely based on trust.

Challenges to the Trust Model



Slide 3

The trust model, however, is coming under pressure as current technological and geopolitical situations evolve. The selling or sharing of personal information is now a lucrative business practice. Furthermore, in response to increased threats of terrorism, governments and law enforcement agencies can now demand access to more and more personal information, and share that information across borders.

With the growth of the Internet, it is now fairly straightforward to compile extensive electronic profiles of individuals. Since this can occur without the individual's knowledge or consent, there is no ability to correct any errors that may be contained in such profiles, and which may have negative consequences for these individuals.

Unauthorized access to these profiles can also result in a host of negative consequences, including identity theft and discrimination.

Alternatives to Trust

- **Emerging role for biometrics**
 - Using physical or physiological characteristics to recognize/authenticate/verify identity
- **May provide:**
 - Added security
 - Stronger authentication
 - Convenience – no need for passwords

www.privacybydesign.ca

Slide 4

In this environment, there is an emerging role for biometrics.

Biometric systems use measurable physical or physiological characteristics or behavioral traits to recognize the identity, or verify/authenticate the claimed identity of an individual.

Biometrics can include fingerprints, iris, face, hand or finger geometry, retina, voice, signature, and keystroke dynamics.

Biometrics: A Primer

Two-Stage Process

1. Enrolment

- Biometric sample is presented; data may be extracted (“biometric template”)
- Biometric sample and/or template are stored

2. Functioning of the system

- Present biometric to the system
- System compares image of submitted sample (or biometric template) against stored biometric data
- If match succeeds, system then “accepts.”

www.privacybydesign.ca

Slide 5

Biometric systems are based on a 2-stage process:

1. A biometric sample is taken from an individual, for instance, a fingerprint or iris scan. This physical characteristic may be presented by an image. Often data are extracted from that sample. These extracted data constitute a biometric template. The biometric data, either the image or the template or both, are then stored on a storage medium. The medium could be a database or a distributed environment, such as smart cards. These preparatory phases together constitute the process of enrolment. The person whose data are thus stored is called the enrollee.
2. The actual purpose of the biometric system is only achieved at a later stage. If a person presents herself to the system, the system will ask her to submit her biometric characteristic(s). The system will then compare the image of the submitted sample (or the template extracted from it) with the biometric data of the enrollee. If the match succeeds, the person is then recognized and the system will “accept” her. If the match does not succeed, she is not recognized and she will be “rejected.”

Privacy and Security Issues in Biometric Systems

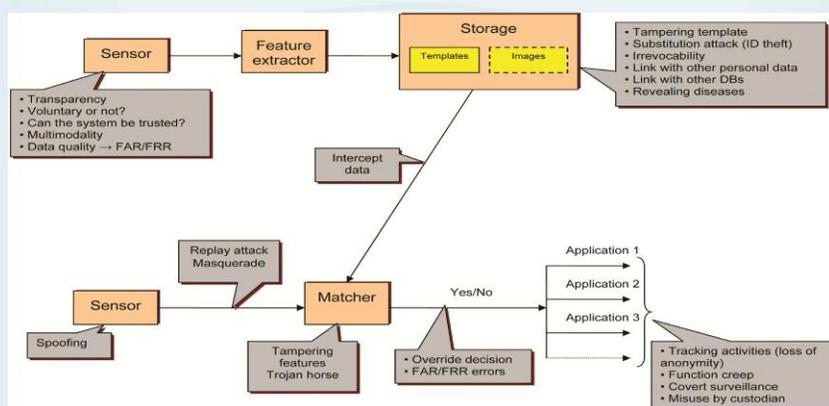


Fig. 1. Privacy and security issues with a biometric system

Slide 6

The collection and use of biometric data, especially for identification purposes, raises a number of privacy and operational issues.

Large centralized databases, accessible over networks in real-time, present significant security and operational risks. If networks fail or become unavailable, the entire identification system collapses. Recognizing this, system designers often build in high redundancy in parallel systems and mirrors to ensure availability. This can increase the vulnerability of the data, since large centralized databases of biometric PII (personally identifiable information), hooked up to networks and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities.

In an effort to preserve maximum compatibility with other fingerprint identification systems, some large-scale biometric identification databases not only collect and file multiple biometric samples but also store the full and complete images of the biometrics involved in addition to the templates.

Storing, transmitting and using biometric images only exacerbates the privacy concerns with large-scale identification systems, since a very important privacy protection afforded by templates is removed, namely, the inability to exactly reconstruct the original biometric image from the template.

Significantly, a compromised biometric can never be replaced. A breach can, therefore, affect individuals for the rest of their lives.

Traditional Biometric Systems: A Dead End for Privacy



Slide 7

The privacy, security, and operational issues associated with biometrics are so significant that biometrics have essentially been a dead end.

The Bottom Line

Traditional Biometrics

Privacy **OR** Security
**A Zero-Sum Equation –
A Win-Lose Proposition**

UNACCEPTABLE!

www.privacybydesign.ca

Slide 8

Many of the challenges associated with biometrics stem from the fact that in traditional biometrics – particularly where biometrics are used for identification purposes – we are forced to choose between security and privacy, which are positioned as being in conflict with one another.

At its core, the issue is that in the traditional approach, the stored biometric template is a unique identifier. This means, in effect, that a database of biometric information is created. Such a database raises significant risks with regard to the potential loss of the biometric, as well as secondary uses. Further, if the database is compromised, the privacy of everyone in the database is impacted. The impact can be very significant, since a person cannot replace their fingerprint, iris scan, or other biometric in the event of a breach.



Slide 9



Slide 10

Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of technologies, business practices, and physical infrastructures. This means building in privacy up front, right into the design specifications and architecture of new systems and processes.

The concept of *Privacy by Design* is predicated on the idea that technology is inherently neutral. As much as it can be used to chip away at privacy, its support can also be enlisted to protect privacy, for example through the use of Privacy-Enhancing Technologies.

How can we apply the principles of *Privacy by Design* to biometrics? Through a technology known as Biometric Encryption (BE)...

Biometric Encryption (BE)

Privacy **AND** Security Positive-Sum Equation – A Win-Win Strategy

www.privacybydesign.ca

Slide 11

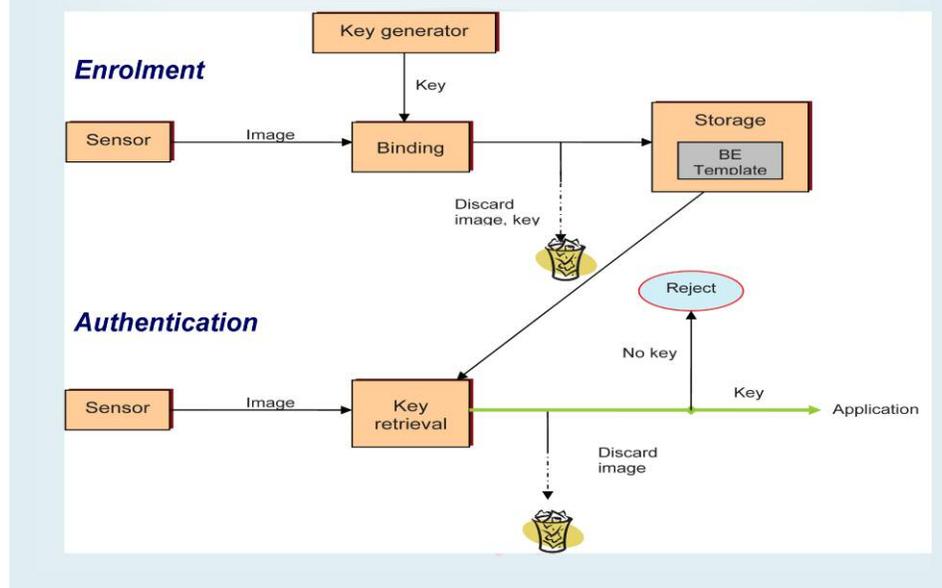
Biometric Encryption (BE) embodies the 7 Foundational Principles of *Privacy by Design*, creating a privacy-enhancing technology that achieves both privacy and security.

BE is a process that securely binds a key to, or extracts a key from, a biometric. It does so in such a way that neither the key nor the biometric can be retrieved from the “helper data” (or “private template”) created and stored through this process, except when the correct live biometric sample is presented for verification.

Since there is no conventional biometric template, there is no stored identifier that can be linked to an identifiable individual. No database of biometric data is created. Instead, the database contains only biometrically encrypted keys. Thus the database as a whole cannot be compromised. If a key is broken, it impacts only the person associated with that key, and the information that is compromised is **not** biometric data.

Biometric Encryption achieves both privacy *and* security, in a positive-sum, win-win model.

Biometric Encryption: Process Overview



Slide 12

This diagram shows how the BE process works.

After a biometric sample is acquired, the BE algorithm securely and consistently binds a key to the biometric to create a protected BE template, also called "private template." In essence, the key *is encrypted* with the biometric. The BE template provides an excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cell phone, etc.). At the end of the enrolment, both the key and the biometric are discarded.

For subsequent verification purposes, the user presents a fresh biometric sample, which, when applied to the legitimate BE template, will let the BE algorithm retrieve the same key/password. In other words, the biometric serves as a *decryption key*. At the end of verification, the biometric sample is discarded once again.

The BE algorithm is designed to account for acceptable variations ("fuzziness") in the input biometric. On the other hand, an attacker, whose biometric sample is different enough, will not be able to retrieve the password.

After the digital key, password, PIN, etc., is retrieved, it can be used as the basis for any physical or logical application. The most obvious use is in a conventional cryptosystem, such as a PKI (Public Key Infrastructure), where the password will generate a pair of Public and Private keys.

Biometric Encryption is an effective, secure, and privacy-friendly tool for biometric password management, since the biometric and the password are bound on a fundamental level.

Advantages of BE over Traditional Biometrics

1. Biometric image/template not retained
2. Multiple/cancellable/revocable identifiers
3. Better authentication security
4. Highly secure personal data and communications
5. Greater compliance with privacy laws
6. Suitable for large-scale applications

www.privacybydesign.ca

Slide 13

1. No retention of biometric image or template

Most privacy and security concerns with traditional biometrics arise as a result of the storage and misuse of biometric data.

2. Multiple/cancellable/revocable identifiers

BE allows individuals to use a single biometric for multiple accounts and purposes without fear that these will be linked together by a single biometric image or template. Account identifiers can also be revoked or changed for newly-generated ones calculated from the same biometric.

3. Improved authentication security; stronger binding of user biometric and identifier

Passwords are bound with the biometric and recomputed directly from it on verification. This results in much stronger passwords that can be longer and more complex, need not be memorized, and are less susceptible to attacks. BE addresses risks associated with traditional biometrics, including substitution attacks, tampering, masquerade attacks, Trojan horses, and overrides.

4. More secure personal data and communications

Users can use BE to encrypt their own personal or sensitive data. Since the key is one's own biometric, BE can place a powerful tool directly in the hands of individuals.

5. Greater compliance with privacy laws

Putting biometric data firmly under the control of the individual, in a way that benefits the individual and minimizes risk of surveillance and identity theft, will go a long way toward satisfying the requirements of privacy and data protection laws, and will promote broader use and acceptance of BE.

6. Suitable for large-scale applications

BE applications align with the preference of privacy and data protection authorities around the world for using biometrics to authenticate or verify identify, rather than for identification purposes alone.

From Theory to Practice

Challenge

The OLG Self-Exclusion Program

- 15,000 + self-excluded people in Ontario
- Need to reliably detect those who attempt to enter a gaming site or casino (manual comparisons do not work!)
- Privacy of all casino patrons must be protected

Solution

Facial recognition in watch-list scenario using Biometric Encryption

Slide 14

The Ontario Lottery and Gaming Corporation (OLG), which runs casinos in Ontario, Canada, approached the province's Information and Privacy Commissioner in 2007 about using facial biometrics to help them identify people entering gaming sites despite having enrolled in a voluntary 'self-exclusion' program for problem gamblers.

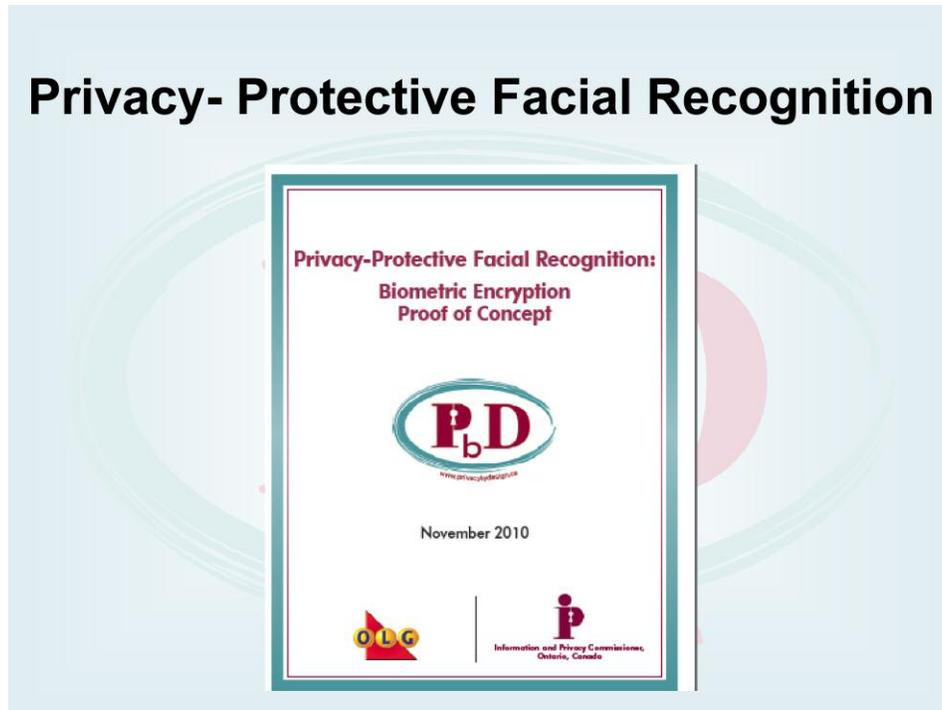
Strong enforcement is a key disincentive for enrollees who may otherwise be tempted to return to gaming sites such as casinos or horse-racing tracks. Until recently, however, enforcement relied largely on a labour-intensive and unreliable manual system of checking photographs.

OLG wanted a new system that would be privacy protective for all casino patrons – those on the list and those not on the list. They knew that biometric systems can raise a number of significant privacy concerns.

Working with the Information and Privacy Commissioner, members of the University of Toronto's Electrical and Computer Engineering Department, and video surveillance/tracking and biometrics firm, iView Systems, OLG was able to practice *Privacy by Design* and explore the application of Biometric Encryption (BE).

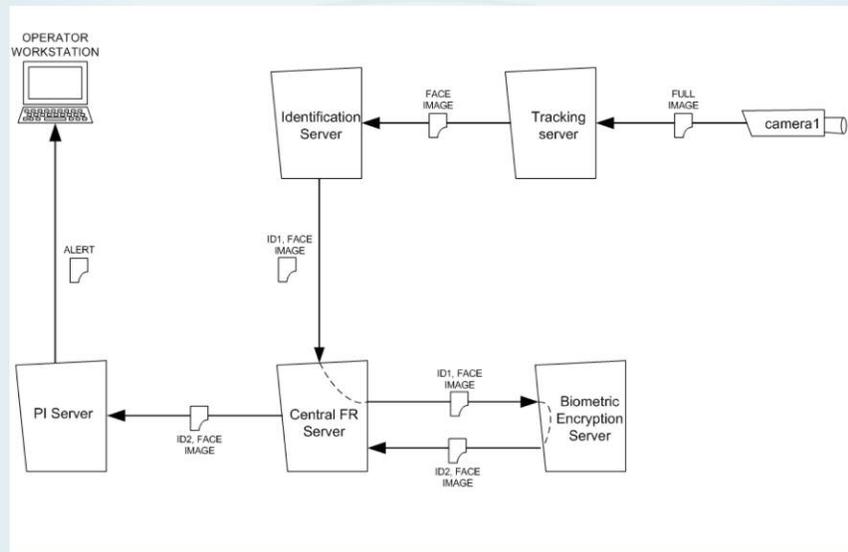
The end goal of this collaboration was to develop a technology that could function in a real-world environment, and would offer dramatically improved privacy protection over simple facial recognition, without compromising functionality, security or performance — the hallmarks of a positive-sum, *Privacy by Design* application.

Privacy- Protective Facial Recognition



Slide 15

Sample Application of BE: Privacy-Protective Facial Recognition



Slide 16

By building privacy in as a requirement from the outset, OLG was able to configure a system using BE that offers not only significant privacy advantages for casino patrons on and off the self-excluded list, but also improves accuracy and enhances system security.

The OLG system will only unlock personal information from the database when the live facial biometric of a self-excluded user is detected as present. As each biometric is only associated with one record, no single key can unlock the complete database.

The diagram here outlines this process, starting on the upper right with the camera icon.

FR= Facial Recognition; PI= Personal Information

Facial Recognition using BE: Key Features

- BE securely binds a person's identifier (the pointer to personal information) with facial biometrics
- The pointer is retrieved only if the right person is present
- The link between facial templates and personal information is controlled by BE
- The final comparison is done manually

Privacy is strongly protected!

Slide 17

The outcome:

- Live field test at Woodbine facilities: Correct Identification Rate (CIR) is up to 91% without BE, and up to 90% with BE – negligible accuracy impact
- BE reduces False Acceptance Rate (FAR) by up to 50% – huge accuracy improvement!
- Accuracy exceeds state-of-the-art for facial recognition
- Triple-win: privacy, security, and accuracy (unexpected) all improved!
- To be deployed in all OLG gaming sites in 2011

Lessons Learned: Benefits of Applying *PbD*

- OLG scenario demonstrates how *Privacy by Design*
 - ✓ Fosters innovation
 - ✓ Improves overall system performance
 - ✓ Makes it possible to achieve *all* system requirements, in a win-win paradigm

www.privacybydesign.ca

Slide 18

More information and a growing library of resources are available at

www.privacybydesign.ca

www.privacybydesign.ca

Slide 19