Applied *Privacy by Design*: Biometric Encryption

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**

Challenges to the Trust Model

Law enforcement access

Electronic dossiers

Hackers

Sale of data

Unauthorized users

Secondary uses

Social Engineering

Identity theft

Deceptive Practices

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

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.”

Privacy and Security Issues in Biometric Systems

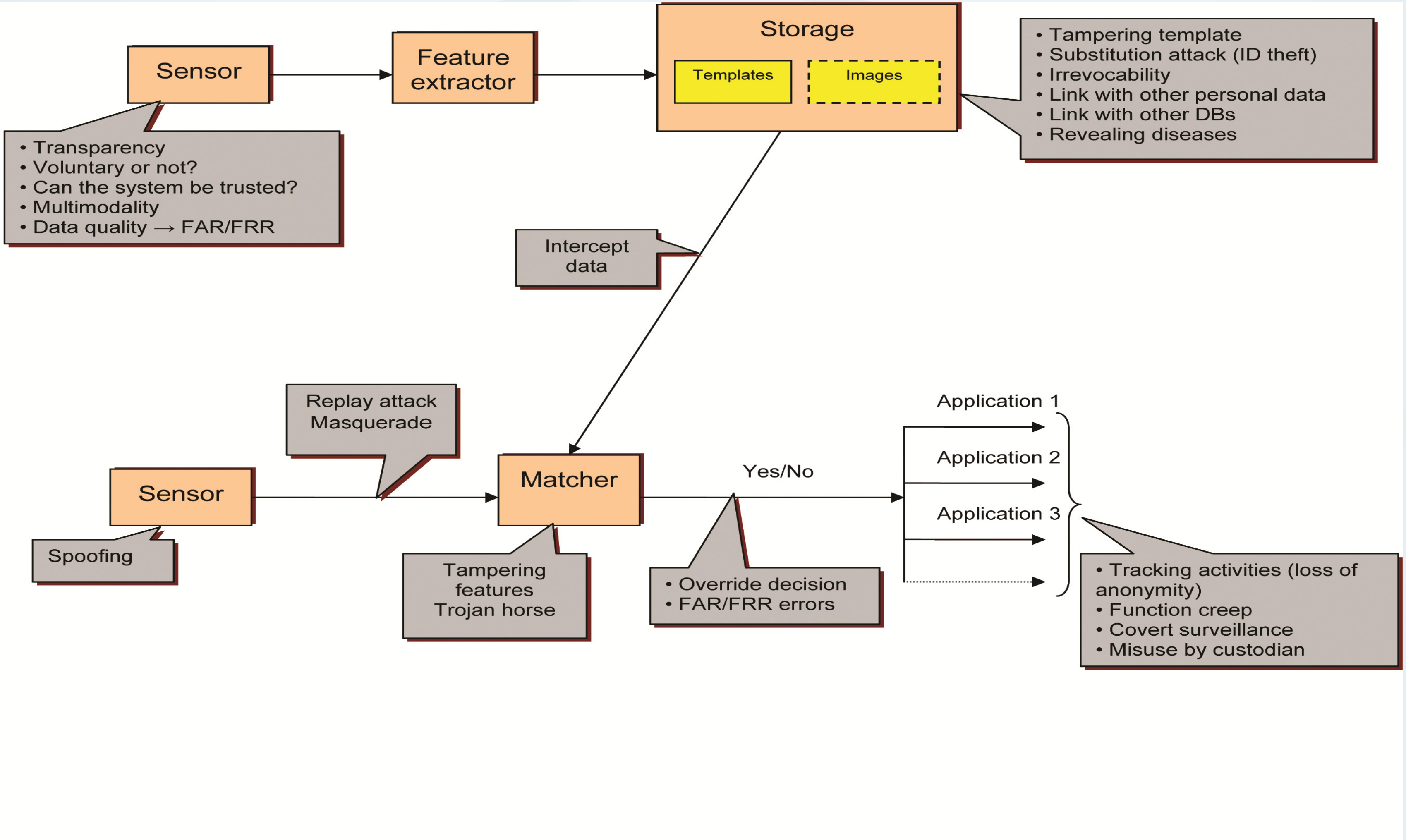


Fig. 1. Privacy and security issues with a biometric system

Traditional Biometric Systems: A Dead End for Privacy

Function creep

Data linkages

Misuse of data

Security risks

Profiling

Surveillance

The Bottom Line

Traditional Biometrics

Privacy **OR** Security

A Zero-Sum Equation –

A Win-Lose Proposition

UNACCEPTABLE!

But there is an alternative….

Privacy by Design

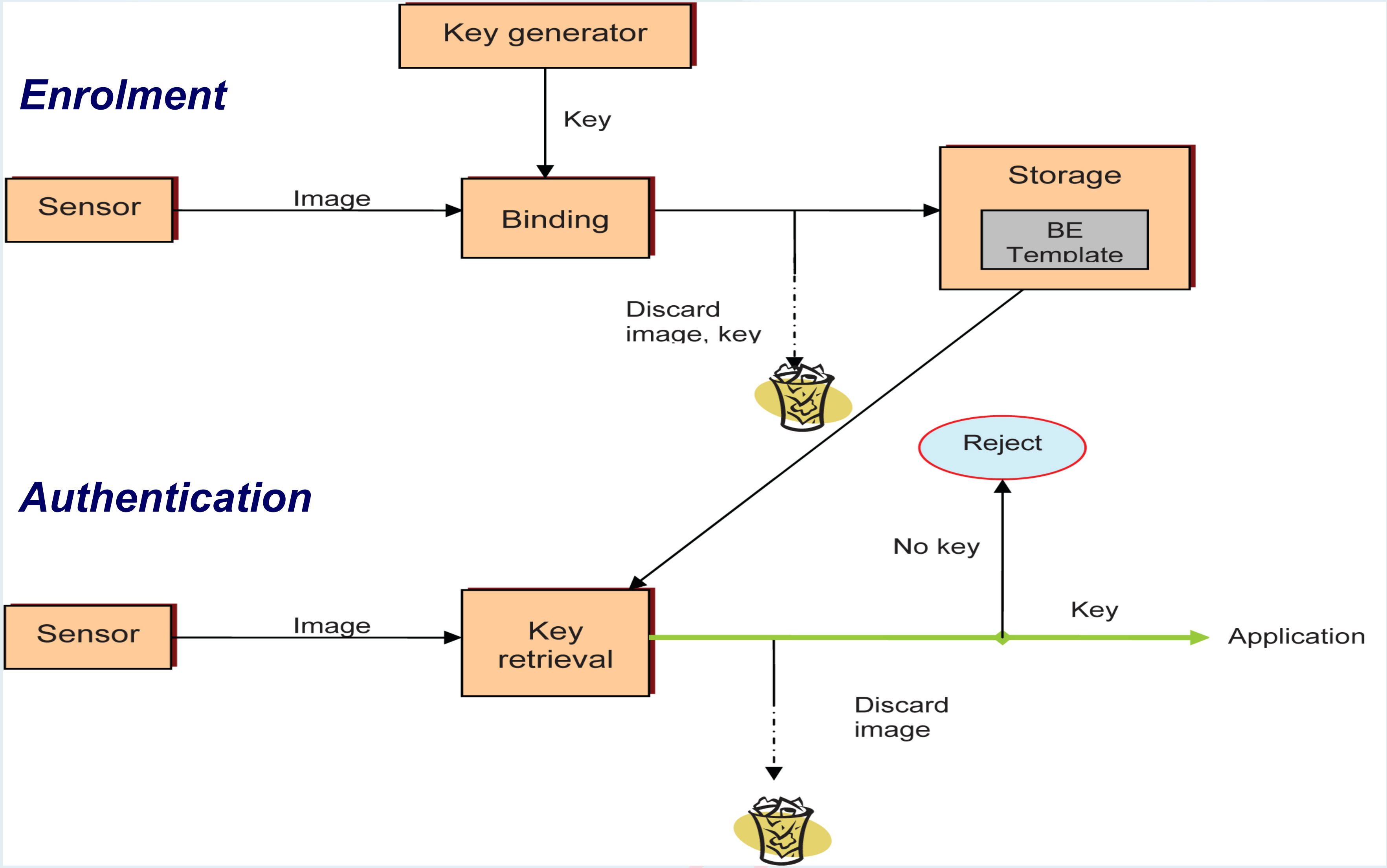
Biometric Encryption (BE)

Privacy **AND** Security

Positive-Sum Equation –

A Win-Win Strategy

Biometric Encryption: Process Overview



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

From Theory to Practice

Challenge

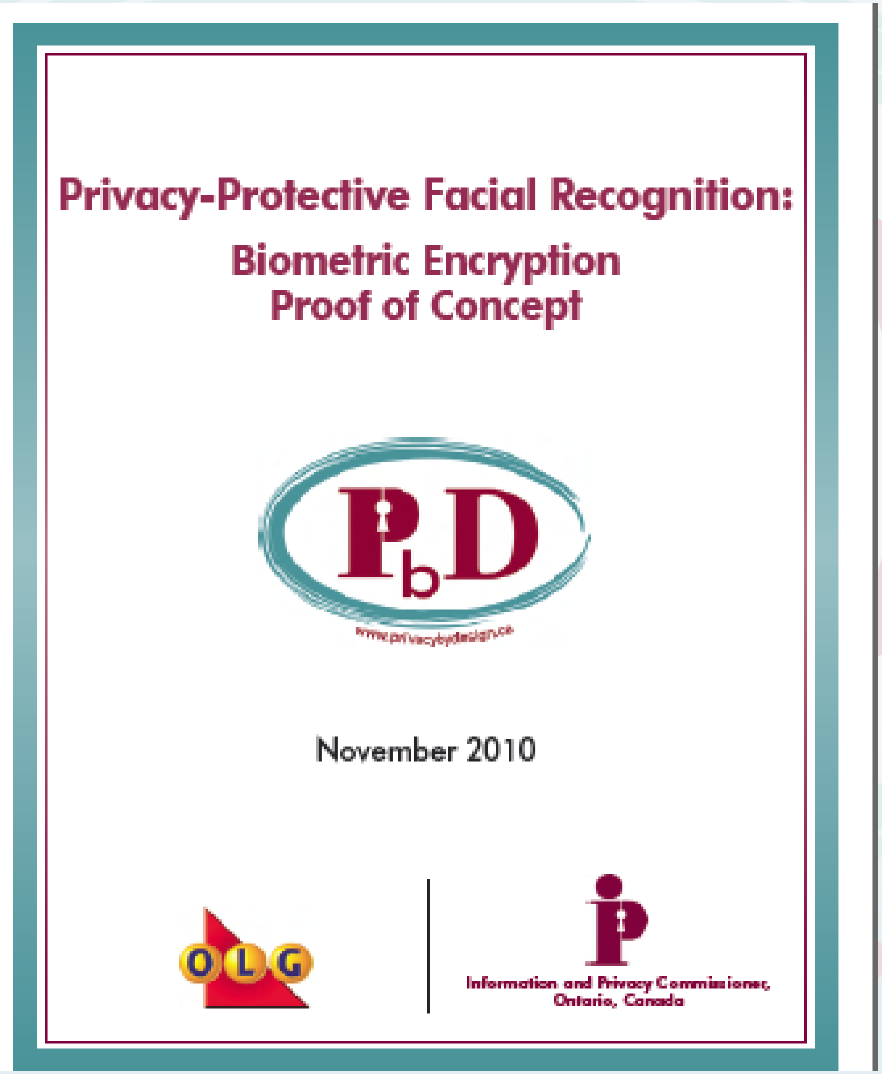
The OLG Self-Exclusion Program

- 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

Privacy- Protective Facial Recognition



Privacy-Protective Facial Recognition:

Biometric Encryption
Proof of Concept

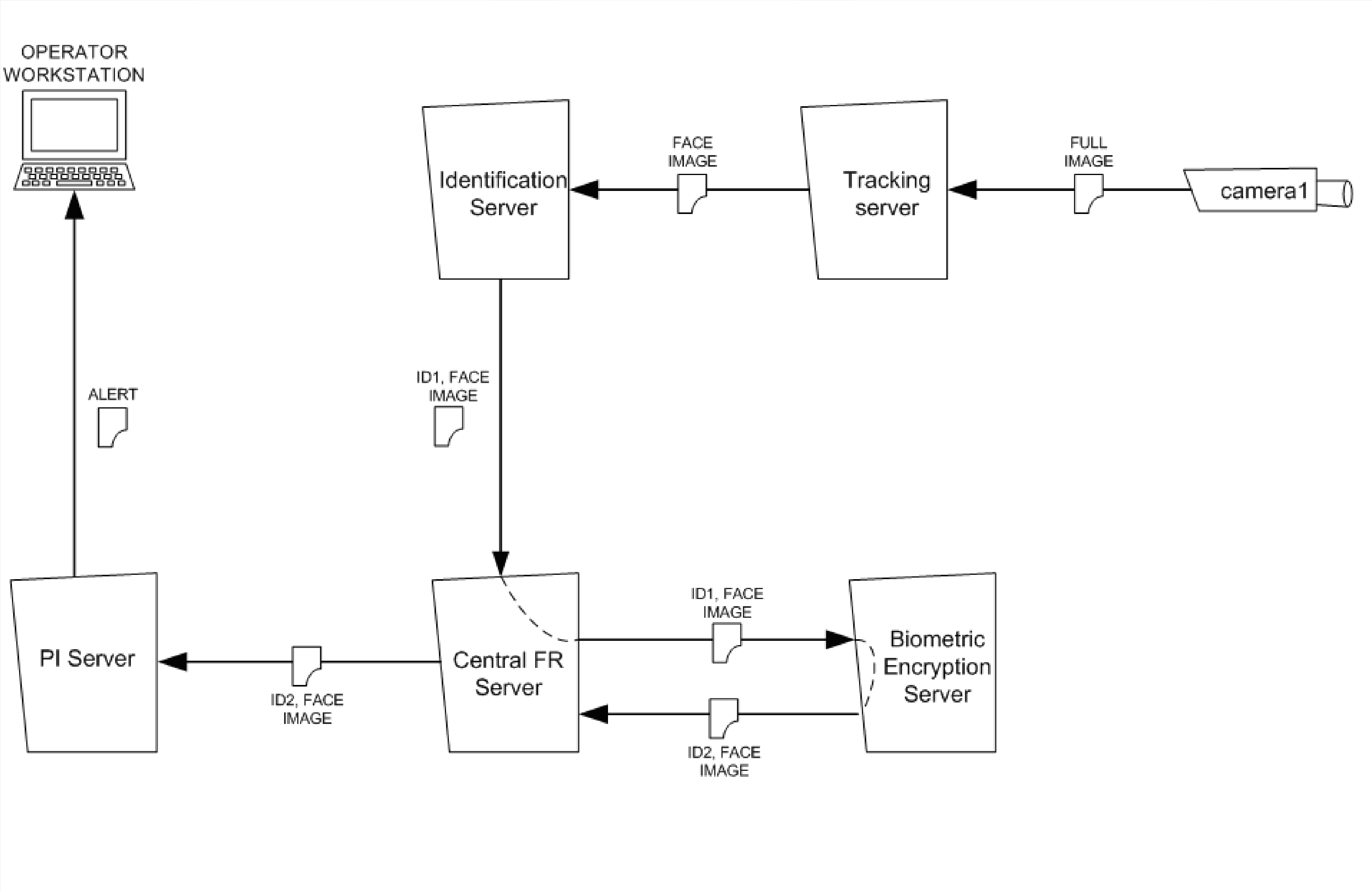
PbD
www.privacybydesign.ca

November 2010

OLG

Information and Privacy Commissioner,
Ontario, Canada

Sample Application of BE: Privacy-Protective Facial Recognition



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!

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

More information and a growing library of resources are available at

www.privacybydesign.ca