



# **Biometric Encryption:** *The Privacy-Enhancing Biometric of Choice*

**Ann Cavoukian, Ph.D.**

**Information and Privacy Commissioner  
Ontario**

**Government of Canada  
Biometrics Working Group  
*July 12, 2007***



# Presentation Outline

1. *Role of the IPC*
2. *Fair Information Practices*
3. *Privacy-Enhancing Paradigms*
4. *Positive vs. Zero-Sum Paradigms*
5. *Biometrics and Privacy*
6. *Untraceable Biometrics: Biometric Encryption*
7. *Current Initiatives*
8. *Biometric Encryption: The Technology*  
— Alex Stoianov, Ph.D.
9. *Conclusion*



# *Role of the IPC*



# Role of the IPC

The role of the Information & Privacy Commissioner of Ontario (IPC) is set out in three statutes:

- *Freedom of Information and Protection of Privacy Act (FIPPA);*
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);*
- *Personal Health Information Protection Act (PHIPA).*



# Mandate of the IPC

**Under its statutory mandate, the IPC is responsible for:**

- investigating privacy complaints;
- resolving appeals from refusals to provide access to information;
- ensuring that organizations comply with the access and privacy provisions of the *Acts*;
- educating the public about Ontario's access and privacy laws; and
- conducting research on access and privacy issues, and providing advice and comment on proposed government legislation and programs.



# Privacy Defined

## **Informational Privacy: Data Protection**

- Personal control over the collection, use and disclosure of recorded information about an identifiable individual;
- An organisation's responsibility for data protection and safeguarding personally identifiable information, in its custody or control.



# What Privacy is Not

**Privacy  $\neq$  Security**



# *Fair Information Practices*



# Fair Information Practices: *A Brief History*

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);
- European Union Directive on Data Protection (1995/1998);
- CSA Model Code for the Protection of Personal Information (1996); Personal Information Protection and Electronic Documents Act (2000);
- United States Safe Harbor Agreement (2000);
- Global Privacy Standard (2006).



# Canada's Fair Information Practices

- **Accountability**
- **Identifying Purposes**
- **Consent**
- **Limiting Collection**
- **Limiting Use,  
Disclosure, Retention**
- **Accuracy**
- **Safeguards**
- **Openness**
- **Individual Access**
- **Challenging  
Compliance**

*CSA Model Code for the Protection of Personal Information*  
(Privacy Code) CAN-CSA Q830 1996

[www.csa.ca/standards/privacy/code/](http://www.csa.ca/standards/privacy/code/)



# Canada's Fair Information Practices

- **CSA Model Privacy Code** was incorporated into Canada's federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) – appended as a schedule;  
[www.privcom.gc.ca/legislation/02\\_06\\_01\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp)
- Organizations that comply with the Privacy Code can be confident that they meet the federal requirements;
- In 2001, the European Commission recognized PIPEDA provides adequate protection for personal data transferred from the EU to Canada.



# Use Limitation Principle

## Use Limitation Principle (OECD):

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:

- i. with the consent of the data subject; or
- ii. by the authority of law.

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

[www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html)



# Limiting Use, Disclosure, and Retention

## Limiting Use, Disclosure, and Retention (CSA)

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except:

- i. with the consent of the individual; or
  - ii. as required by law.
- Personal information shall be retained only as long as necessary for the fulfillment of those purposes.



# Global Privacy Standard

- In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners convened for the sole purpose of creating a single Global Privacy Standard (GPS);
- Globalization and converging business practices created a need to harmonize various sets of fair information practices so that businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually enhancing privacy;
- The GPS builds upon the strengths of existing codes containing time-honoured privacy principles and reflects an enhancement by explicitly recognizing the concept of “data minimization” under the “collection limitation” principle;
- The final version of the GPS was formally tabled and accepted by Commissioners in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.



# Global Privacy Standard

## *Use Limitation Principle*

### **GPS Privacy Principle # 5**

#### **Use, Retention, and Disclosure Limitation:**

Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.



# *Privacy-Enhancing Paradigms*



# Privacy-Enhancing Technologies (*PETs*)

- The IPC coined the concept and methodology recognized around the world today as *privacy-enhancing technologies* (PETs);
- In 1995, the IPC and the Dutch Data Protection Authority published the landmark study, *Privacy-Enhancing Technologies: The Path to Anonymity (Vols. I & II)*.



# Privacy-Enhancing Technologies (*PETs*)

- Privacy Enhancing Technologies include those that empower individuals to manage their own identities in a privacy enhancing manner.
- These include tools or systems to:
  - anonymize and pseudonymize identities;
  - securely manage login ids and passwords and other authentication requirements;
  - restricts traceability and limits surveillance;
  - allow users to selectively disclose their PII to others and exert maximum control over their PII once disclosed.



# Privacy by Design

*“Technology knows no borders;  
... transcends jurisdiction.”*

- This has been the driving force behind my office’s approach to privacy, in shaping public policy and organizational practices, on a wide range of technology-related issues, including:
- RFIDs, biometrics, smartcards, PKI, DRM, P3P, identity management systems, video surveillance, national ID cards, electronic road toll systems, and Social Networks (Facebook).



# “Build It In”

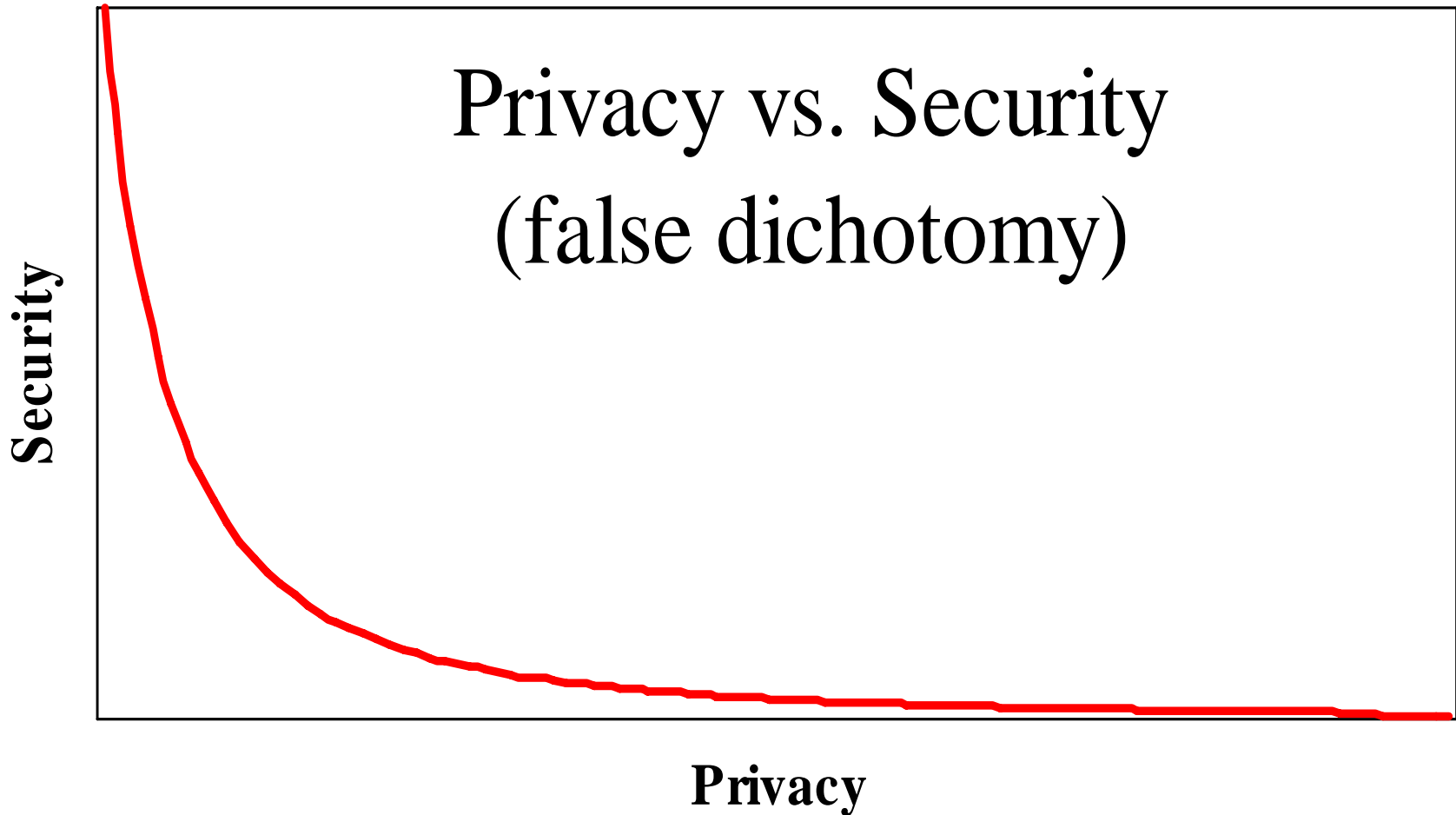
- Build in privacy – up front, into the design specifications into the architecture; if possible embed privacy right into the technology used – *bake it in*;
- Assess the risks to privacy: conduct a privacy impact assessment; follow up with annual privacy audits;
- Data minimization is key: minimize the routine collection and use of personally identifiable information – use encrypted or coded information whenever possible;
- Use privacy enhancing technologies (PETs): give your customers maximum control over their data.



# *Positive vs. Zero-Sum Paradigms*



# Privacy OR Security: *A Zero-Sum Game*



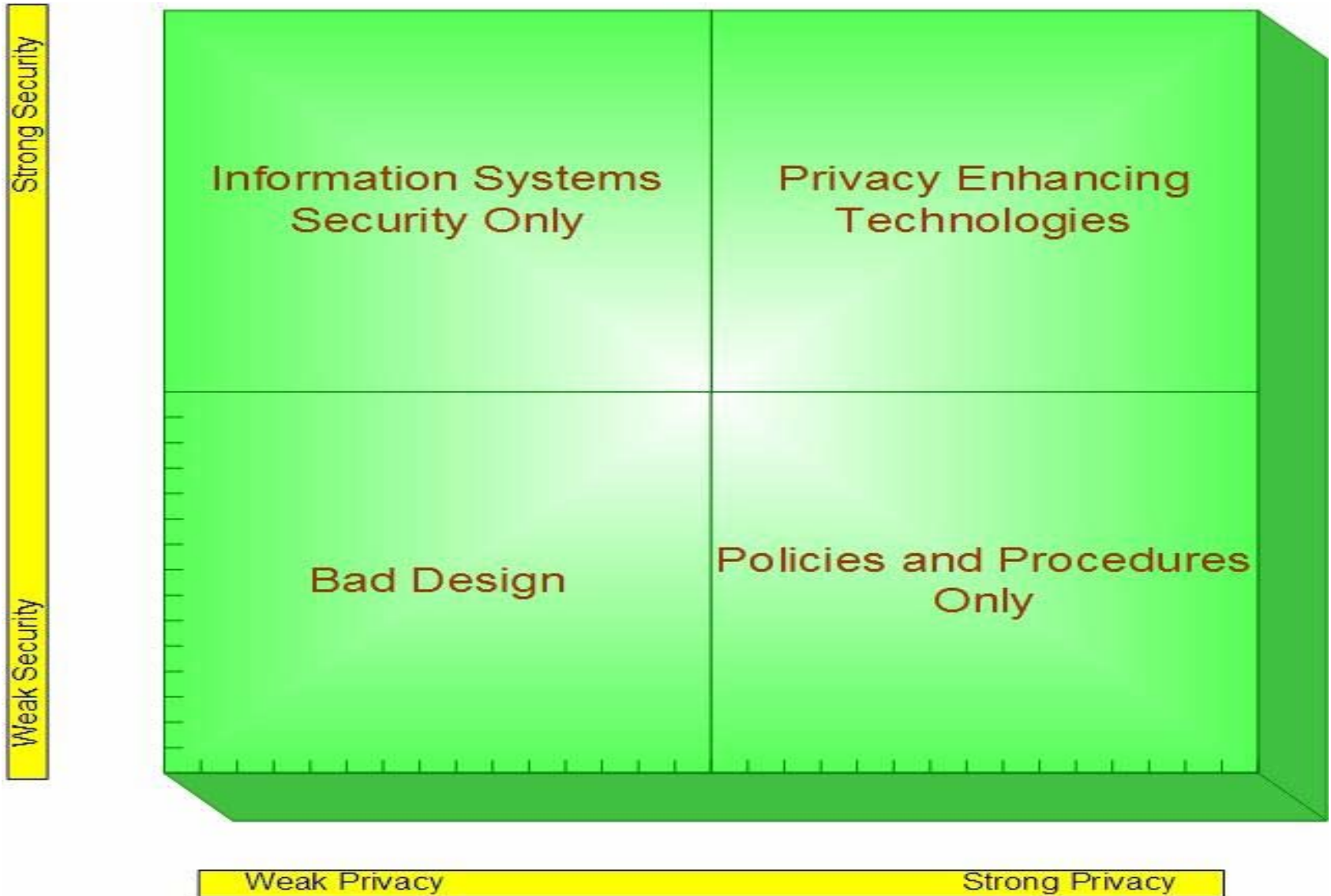


# Positive-Sum Model

*Change the paradigm  
from a zero-sum to  
a positive-sum model*



# Privacy AND Security





# September 11, 2001

*“Public safety is paramount but  
balanced against privacy”*

- Security measures must be real, not illusory;
- New powers must be studied and measured to determine their effectiveness and utility;
- Are new security powers truly necessary or are existing ones not fully utilized or effectively deployed?

[www.ipc.on.ca/userfiles/page\\_attachments/1517136\\_pub01-e.pdf](http://www.ipc.on.ca/userfiles/page_attachments/1517136_pub01-e.pdf)

[www.cbc.ca/news/indepth/usattacked/essay\\_privacy.html](http://www.cbc.ca/news/indepth/usattacked/essay_privacy.html)



# *Biometrics and Privacy*



# Growth of Biometrics

- CANPASS – Facilitates efficient and secure entry into Canada by allowing pre-approved travelers to meet their border clearance obligations by simply looking into a camera that recognizes the iris of the eye as proof of identity;
- NEXUS – A Canadian joint program with U.S. Customs designed to expedite the border clearance process for low risk, pre-approved travelers;
- International Civil Aviation Organization approved facial recognition for travel documents;
- EU to implement biometrics in passports and visas;
- AAMVA Unique Identifier Working Group;
- BioPay LLC – developing and implementing a biometric payment system for retail stores in the U.S.;
- Biometric technologies are beginning to be utilized in U.S. and U.K. schools for library services, vending machines, class attendance and tuition payments;
- Several countries are in the process of developing and implementing programs for biometrically enhanced National ID cards.



# Proposed Biometrics Program, City of Toronto

- In 1994, the City of Toronto, Canada, was planning to introduce encrypted finger scanning technology in an attempt to combat fraud in the welfare/social assistance system – double dipping;
- My office (IPC) took the lead in ensuring that if biometric technology was to be used, the most privacy protective technology had to be used, with extensive, legislated safeguards;
- The IPC developed a list of procedural and technical safeguards that formed the standard that had to be met by whatever technology was adopted;
- The IPC worked closely with the Ministry of Social Services to ensure that the above safeguards were enshrined in legislation, resulting in the *Ontario Works Act, 1997*.



# European Biometrics Forum

- The European Biometrics Forum (EBF) was launched in 2003 – invited to speak at their inaugural conference in Dublin;
- Asked to become a member of the International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometric industry to strengthen trust and confidence in the use of emerging biometric applications;
- The EBF is supported by a network of national biometric organizations, companies, universities and experts across Europe in carrying out research for the development of a roadmap for the European Biometrics industry from 2003-2010.



# IPC and Biometrics

- Biometrics Program, Toronto (1994)
- Biometric Encryption concept lauded (1996)
- *Ontario Works Act* (1997)
- Discussion and guidance papers (1999)
- Presentations, speeches, etc. (2000 to present)
- Statement to House of Commons Standing Committee on Citizenship & Immigration (2003)
- Resolution of Int'l DPAs (2005)
- EBF IBAC (2005 to present)



# Privacy and Biometrics:

## *The Risks*

- Creation of large centralized databases containing biometric templates (that may then be linked together);
- Far-reaching consequences of errors in large-scale networked systems;
- Interoperability that invites unintended additional “secondary” uses (contrary to the Use Limitation Principle).



# Privacy and Biometrics

## *Issues*

- Expanded surveillance;
- Diminished oversight;
- Absence of knowledge or consent;
- Loss of personal control;
- Loss of Use Limitation Principle (Function Creep).



# Biometric Applications

- **Identification:**
  - one-to-many comparison;
- **Authentication/Verification:**
  - one-to-one comparison.



# Centralized Databases

- Risks associated with large centralized, networked biometric databases;
- Article 29 Working Party, chaired by Peter Schaar, Germany's federal Data Protection Commissioner, EU Opinion, August 2004 states, "*The Working Party strictly opposes the storage of all EU passport holders' biometric and other data in a centralized data base...*"

[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp112\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_en.pdf)



# Interoperability

- Interoperable biometric databases invite additional purposes and secondary uses of the data;
- E.U. Data Protection Supervisor, Peter Hustinx, in his March 2006 Opinion, stressed that:

*“Interoperability of systems must be implemented with due respect for data protection principles and in particular, the purpose limitation principle.”*

Comments on the Communication of the Commission on interoperability of European databases, [www.edps.eu.int/legislation/Comments/06-03-10\\_Comments\\_interoperability\\_EN.pdf](http://www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf)



# Authentication/Verification: *Biometric Strength and Privacy*

The strength of one-to-one matches:

- Authentication/verification does not require the central storage of biometric templates;
- Biometric may be stored locally, not centrally – on a smart card, token, travel document, etc. – and then compared to the live sample.



# 1:1 versus 1:Many

- Privacy regulators favor 1:1 authentication (verification) over 1:many identification;
- The EU Article 29 Working Party Resolution on the use of biometrics in passports, identity cards and travel documents was passed by Data Protection and Privacy Commissioners in Montreux, Switzerland, 2005:

*“...The Conference calls for the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder, when presenting the document.”*

— 27th International Conference of Data Protection and Privacy Commissioners,  
Montreux, 16 September 2005

[www.privacyconference2005.org/fileadmin/PDF/biometrie\\_resolution\\_e.pdf](http://www.privacyconference2005.org/fileadmin/PDF/biometrie_resolution_e.pdf)



*Untraceable  
Biometrics:  
Biometric Encryption*



# Biometric Encryption (BE)

## What is Biometric Encryption?

- Class of emerging “untraceable biometric” technologies that seek to transform 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” (untraceable) labeling of sensitive records (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.



# Advantages of Biometric Encryption

## **BE Embodies core privacy practices:**

1. Data minimization: no retention of biometric images or templates, minimizing potential for unauthorized secondary uses, loss, or misuse;
2. Maximum individual control: Individuals may restrict the use of their biometric data to the purpose intended, thereby avoiding the possibility of secondary uses (function creep);
3. Improved security: authentication, communication and data security are all enhanced.



# IPC Objectives

- Stimulate demand for PETs: Bring this privacy-enhancing biometric technology to the attention of the public, government, policymakers, industry – showing that it *is* possible and should be considered;
- Stimulate supply of PETs: Encourage research, development and commercialization of privacy-enhancing technologies as viable solutions for real-world applications.



# *Current Initiatives*



# Current Initiatives

## University of Toronto:

- Identity, Privacy and Security Initiative (Chair, Advisory Council);
- Preparing a tutorial for M. Eng Seminar Series;
- Preparing a tutorial for IEEE and an article for IEEE publication;
- Writing a chapter on Biometric Encryption for academic textbook: *Biometrics: Fundamentals, Theory and Systems*.



# Current Initiatives (Cont'd)

## **Bell Canada:**

- Exploring a pilot project regarding BE and voice biometrics for customer authentication;

## **IBM:**

- Partnering on a research project regarding privacy-enhancing biometrics;

## **Phillips:**

- Exploring the use of Evaluation Licences of their BE algorithm in various applications.



# ***Biometric Encryption: The Technology***

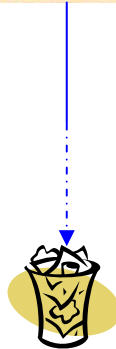
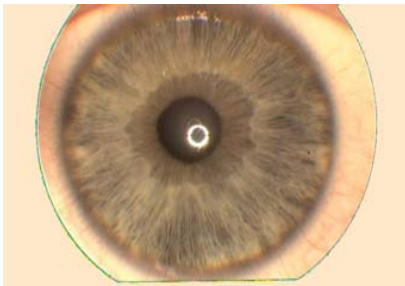
**— Alex Stoianov, Ph.D.  
Biometrics Specialist, IPC/Ontario**



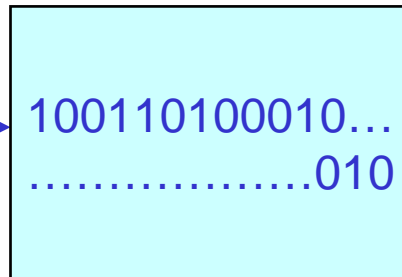
# Use Biometric as the Encryption Key

Enrollment

Biometric Image



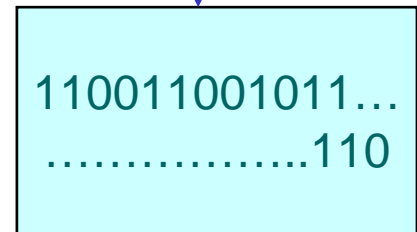
Biometric Template



Randomly generated key



BE binding algorithm

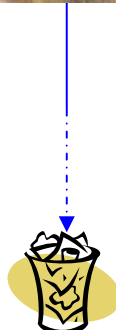
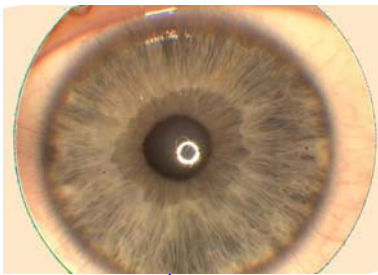


Biometrically-encrypted key is stored

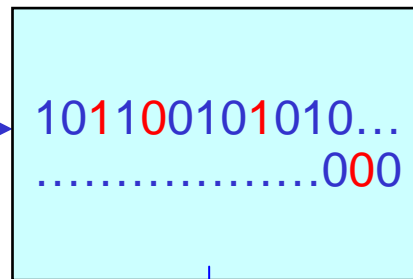
# Decrypt with Same Biometric

Verification

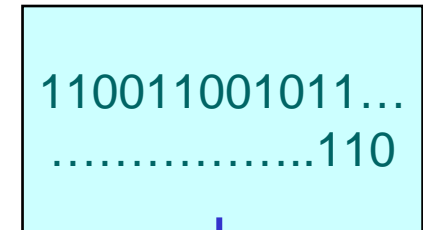
Fresh Biometric Image



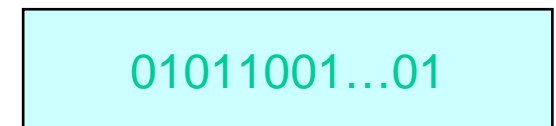
Fresh Biometric Template



Biometrically-encrypted key



BE retrieval  
algorithm



Key retrieved



# Fuzzy Commitment Scheme for Iris

*(Hao, Anderson, Daugman 2005)*

Enroll

Iris template, 2048 bits:

100110100010.....010

140-bit key:

01011001...01

Map to 2048-bit ECC codeword:

010101101001.....100

XOR:

110011001011.....110

Store as a biometrically-encrypted key



# Fuzzy Commitment Scheme for Iris

*(Hao, Anderson, Daugman 2005)*

Verify

Fresh iris template, 2048 bits:

101100101010.....000

Retrieve biometrically-encrypted key:

110011001011.....110

XOR:

0111110001.....110

If the number of errors is within the ECC bound, the ECC will decode the correct 140-bit key:

01011001...01



# BE Technologies

- Fuzzy Commitment/Fuzzy Extractor scheme:
  - Philips privID™ : face, fingerprints, iris;
  - Hao, Anderson, Daugman: iris;
- Mytec BE: fingerprints;
- Fuzzy Vault: fingerprints;
- Biometrically hardened passwords (Monrose et. al):  
keystroke dynamics, voice;
- Other terms: biometric “cryptosystem,” private template, biometric signature, secure sketch, biometric locking, virtual PIN.

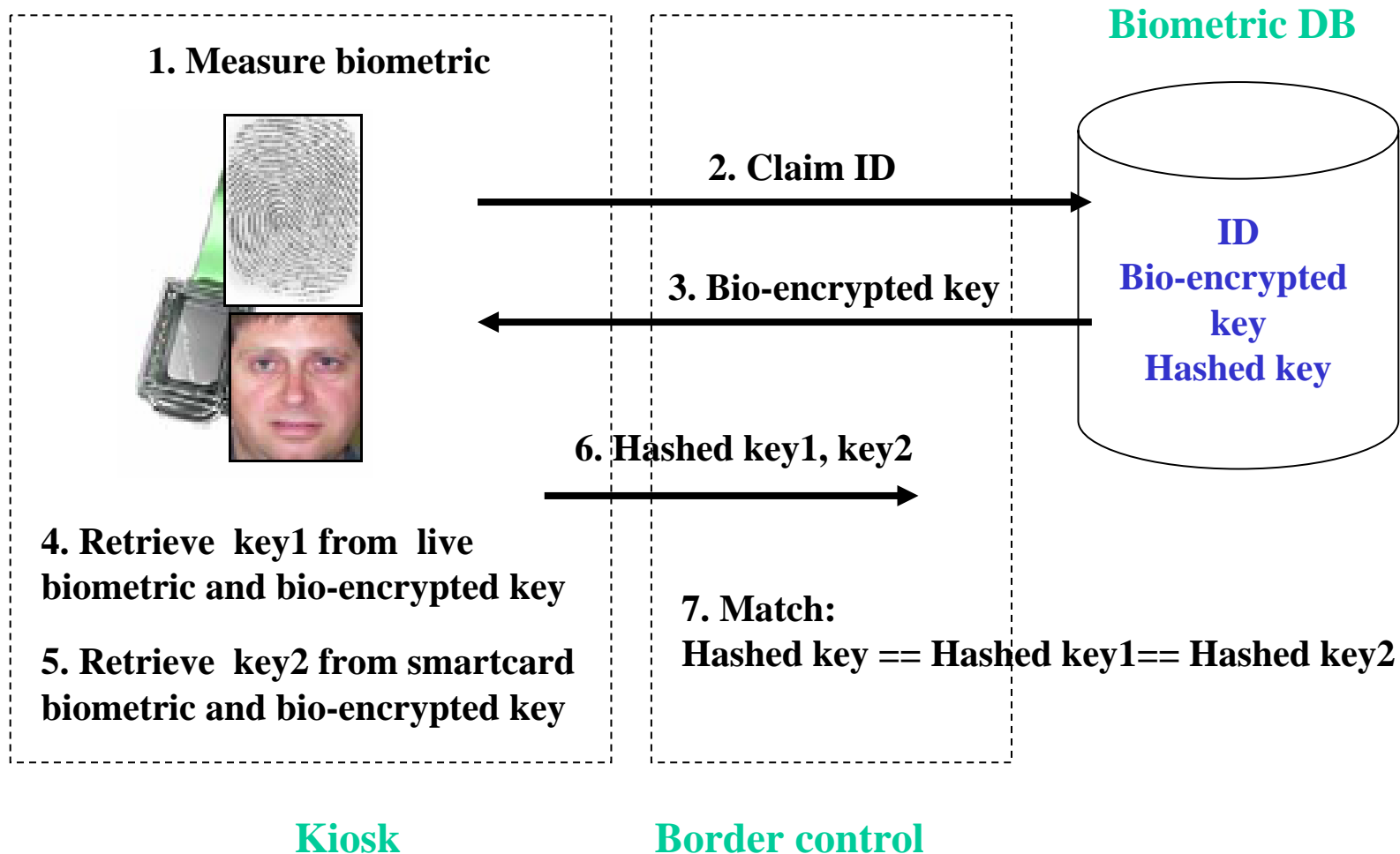


# BE Case Scenarios Described in Paper

1. Small-scale use  
(personal authentication);
2. Anonymous (untraceable) database  
(access to hospital records);
3. Travel documents  
(3-way checks).



# Three-way-Check in the ePassport Scenario (Philips)





# *Conclusion*



# Conclusion

- We need to change the paradigm away from a zero-sum to a positive-sum model where both privacy and security are built into biometric technologies;
- Honouring the “Use Limitation Principle” found in Fair Information Practices will gain the respect and support of privacy commissioners worldwide;
- The use of privacy-enhancing biometrics such as Biometric Encryption will ensure that the “Use Limitation Principle” is respected and that privacy is protected, while at the same time, delivering strong security – a true win/win scenario.



# How to Contact Us

**Ann Cavoukian, Ph.D.**

**Information and Privacy Commissioner 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](http://www.ipc.on.ca)**

**E-mail: [info@ipc.on.ca](mailto:info@ipc.on.ca)**