Biometric Encryption:

A Transformative Technology that Delivers Strong Security and Privacy

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Institute of Electrical and Electronics Engineers

6th Biometrics Symposium

September 23, 2008

Presentation Outline

1. *The Privacy Landscape: Privacy "101"*
2. *"Privacy by Design"*
3. *"Transformative Technologies"*
4. *Biometrics and Privacy*
5. *Biometric Encryption*
6. *"Radical Pragmatism"*
7. *Conclusions*

Please accept my apologies for not being able to join you here in person today – an emergency surgery made it unavoidable. But I'm here in spirit – and my spirit is going "radical," but in a pragmatic way! Hold on to your seats as you hear about our new "Radical Pragmatism."

… See you next time,

Ann Cavoukian, Ph.D.
Commissioner

The Privacy Landscape: Privacy "101"

Privacy = Freedom

What Privacy is Not

Privacy ≠ Security

Privacy and Security:
The Difference

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Security:

Organizational control of information through information systems

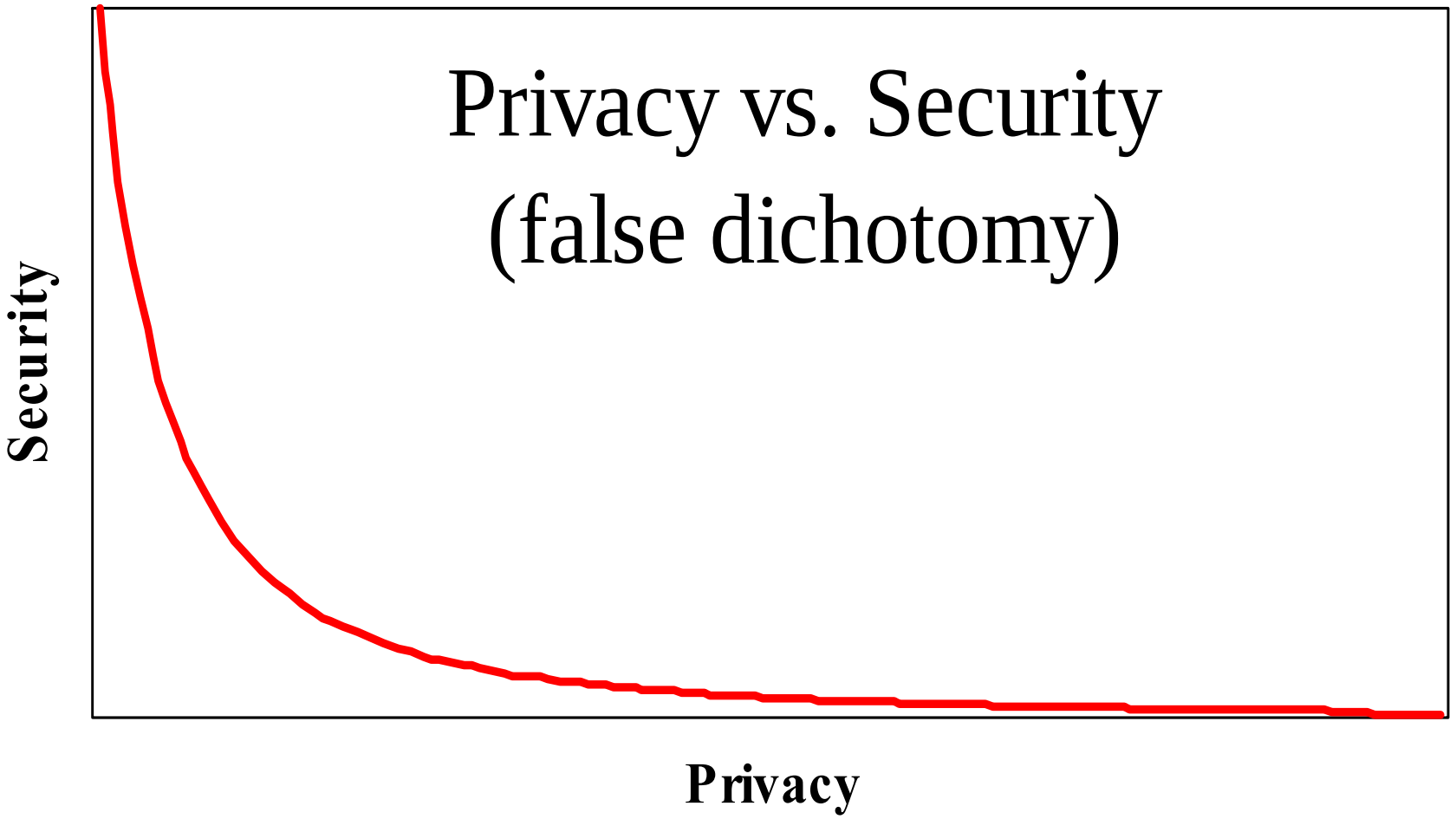
- Privacy; Data Protection
- Fair Information Practices
- “Use” of Personally Identifiable Information (PII)

Information Privacy Defined

Information Privacy: Data Protection

- Freedom of choice; personal control; informational self-determination;
- Control over the collection, use and disclosure of any recorded information about an identifiable individual;
- Privacy principles embodied in "Fair Information Practices."

Privacy OR Security:
A Zero-Sum Game



Change Your Perception of Privacy and Technology

I want you to think differently …

Change the Paradigm!

Think
“Positive-Sum”
Not Zero-Sum

Positive-Sum Paradigm

- A **Zero-Sum Paradigm** describes a concept or situation in which one party's gains are balanced by another party's losses – win/lose; either/or; enhancing security comes at the expense of privacy – the more you have of one, the less you can have of the other;
- A **Positive-Sum Paradigm** describes a situation in which *all* participants may gain together (win-win);
- To achieve a positive-sum model, privacy must be proactively built into the system, so that privacy protections are engineered directly into the technology, right from the outset;
- The effect is to minimize the unnecessary collection and use of personal data by the system, while at the same time, strengthening data security, and empowering individuals to exercise greater control;
- This can result in technologies that achieve strong security *and* privacy, delivering a "win-win" outcome.

Positive-Sum Model

Change the paradigm
from a zero-sum to
a positive-sum model:
Create a "win-win" scenario,
not an "either/or"
involving unnecessary
trade-offs

"Privacy by Design"

Privacy by Design: "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.

The Next Wave: "Transformative Technologies"

Background: 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).*

  Vol. I - www.ipc.on.ca/index.asp?layid=86&fid1=329

  Vol. II - www.ipc.on.ca/images/Resources/anoni-v2.pdf

Privacy-Enhancing Technologies *(PETs)*

- Privacy Enhancing Technologies enlist the support of technology to **protect** privacy. They include those that empower individuals to manage their own identities and personally-identifiable information (PII) in a privacy enhancing manner – encryption plays a key role.
- These include tools or systems to:
  - anonymize and pseudonymize identities;
  - securely manage login ids and passwords and other authentication requirements;
  - restrict traceability and limit surveillance;
  - allow users to selectively disclose their PII to others and exert maximum control over their PII once disclosed.

Time to Move Forward …

… from PETs to Trans Tech

Transformative Technologies

Surveillance Technology + Positive-Sum Paradigm + Privacy Enhancing Technology = Transformative Technologies

Common characteristics of Transformative Technologies:

- Help minimize unnecessary disclosure, collection, retention and use of personal data;
- Empower individuals to participate in the management of their personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in (personal) data governance structures;
- Help promote and facilitate widespread adoption of those technologies.

Privacy = Freedom

Biometrics and Privacy

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.

www.eubiometricforum.com

TURBINE

(TrUsted evocable Biometric IdeNtitiEs)

- BE is the focus of a large EU research project, TURBINE (TrUsted evocable Biometric IdeNtitiEs), that is currently being funded by the European Union's (EU) 7th Research and Development Framework Program;
- TURBINE aims to develop biometric identity solutions that combine automatic fingerprint recognition and cryptographic techniques, but its primary objective is to prove that such technologies are commercially viable;
- The EU's funding of TURBINE is a huge endorsement of BE's potential for large-scale applications, and also validation that privacy has a legitimate place in the debate regarding international security regimes.

IPC and Biometrics

- IPC Publication: *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (2007)
- EBF IBAC (2005 to present)
- Resolution of Int'l DPAs (2005)
- Statement to House of Commons Standing Committee on Citizenship & Immigration (2003)
- *Ontario Works Act* (1997)
- Biometrics Program, Toronto (1994)

Biometric Applications

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

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

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

Misleading Statements from Biometrics Vendors

- "The stored biometric information is just a meaningless number" (i.e. it is not Personally Identifiable Information);
- "The biometric templates stored in our database cannot be linked to other databases because we use a proprietary algorithm;"
- "A biometric image cannot be reconstructed from the stored biometric template."

Biometric Encryption

Biometric Encryption (BE)*

What is Biometric Encryption?

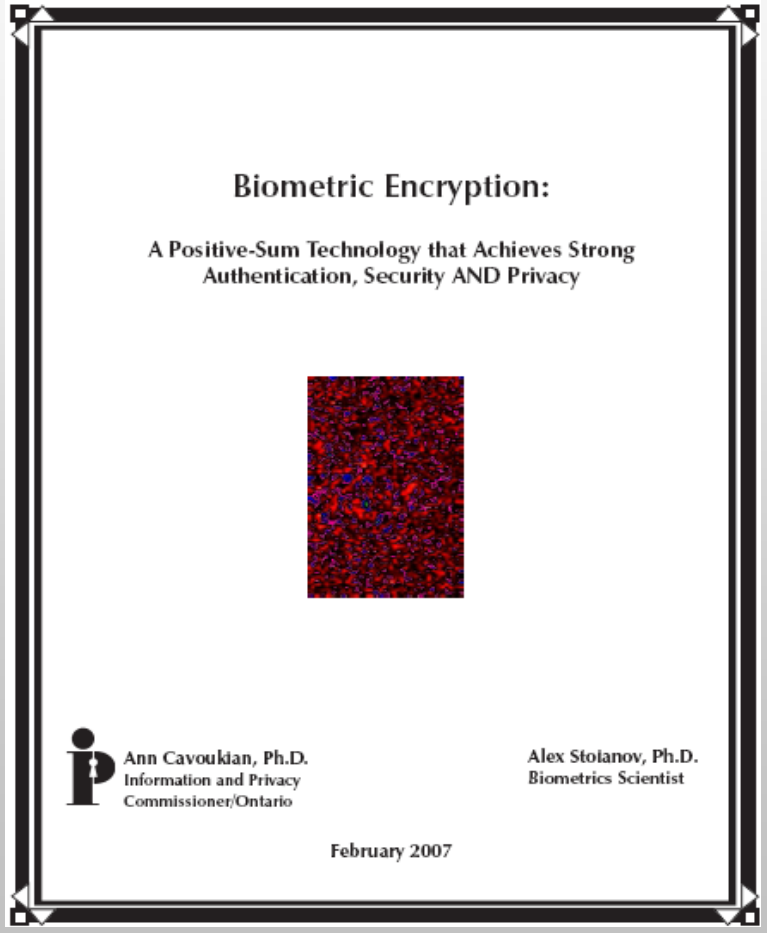
- Class of emerging “untraceable biometric” technologies that seek to transform the biometric data provided by the user;
- Special properties:
  - uniqueness
  - irreversibility

* Pioneering development by George Tomko, Ph.D. Founder of Mytec Technologies,1994.

Biometric Encryption:

A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy

- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of BE over other uses of biometrics;
- How BE technology can help to overcome the prevailing "zero-sum" mentality by effectively transforming one's biometric to a private key.



www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

Advantages of Biometric Encryption

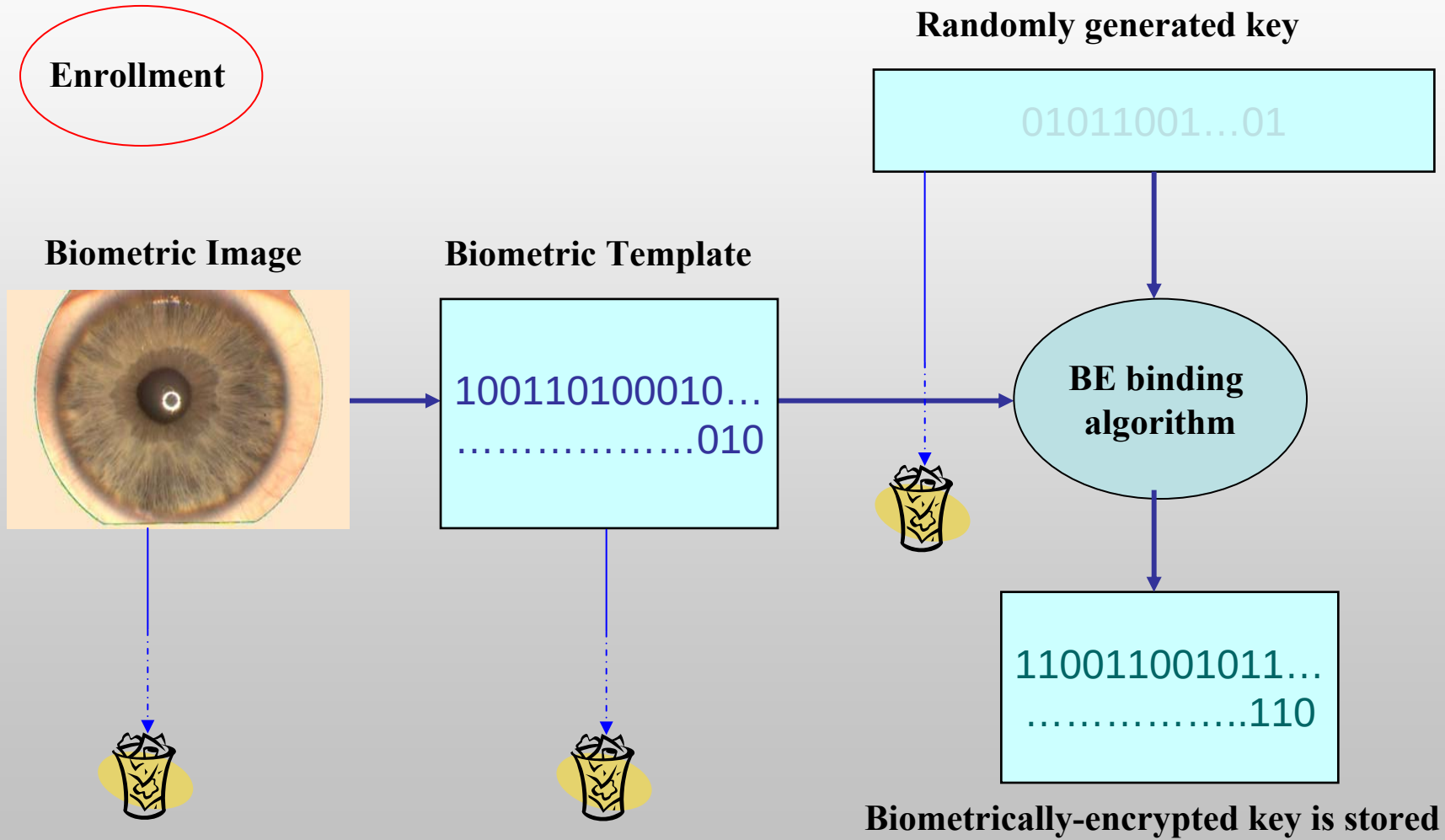
BE Embodies core privacy practices:

1. Data minimization: no retention of biometric images or templates, minimizing potential for unauthorized secondary uses, loss, or misuse;

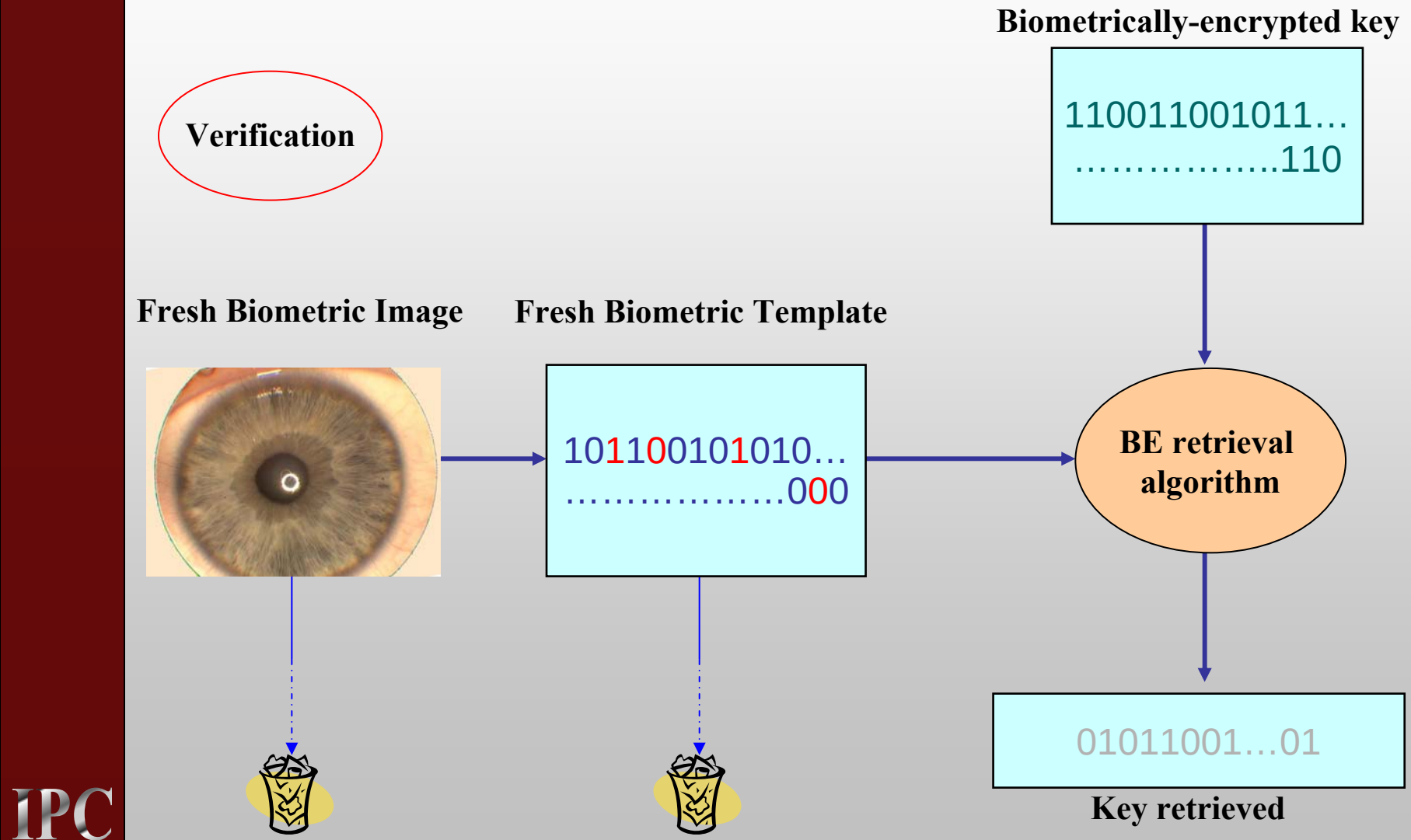
2. Maximum individual control: Individuals may restrict the use of their biometric data to the purpose intended, thereby avoiding the possibility of secondary uses (function creep);

3. Improved security: authentication, communication and data security are all enhanced.

Use Biometric as the Encryption Key



Decrypt with Same Biometric



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.

Current BE Projects

- **The Philips privID™ (Netherlands) –** is currently one of the most advanced BE technologies in operation; unlike some BE systems, the privID™ system is very fast which allows for a true one-to-many mode; it is also very secure, making it extremely difficult to crack;
- **PerSay (Israel) –** has successfully combined their own voice authentication technology with Philips' BE technology making voice biometric encryption a reality. A major telecommunications company is now exploring the possibility of deploying a voluntary voice identity verification service for its customers using this new technology;

Current BE Projects (Cont'd)

- **University of Toronto –** Professor Kostas Plataniotis and Karl Martin have developed a privacy-enhancing approach to video surveillance cameras using cryptographic techniques to secure a private object (face/image), so that it may only be viewed by designated persons, by unlocking the encrypted object with a secret key. The Toronto Transit Commission is now exploring the possibility of using this technology for their video surveillance system;
- **Ontario Lottery and Gaming Corporation** (OLG) is exploring the use of facial biometrics to assist gamblers who voluntarily choose, under the self-exclusion program, to provide photos of themselves so that they may be denied entry into casinos, at their own request, due to their gambling addictions.

“Radical Pragmatism”

Radical Pragmatism

Radical

Radical

(/raedikel/ adj, & n.) — adj.

2) **far-reaching … thorough.**

— Concise Oxford Dictionary, Eighth Edition, 1990.

Radical Privacy Pragmatism

Radical = far-reaching … thorough;

Pragmatism ≠ status quo;

Radical Pragmatism (in the area of privacy)
is the embodiment of a positive-sum paradigm,
involving a practical approach,
invoking the need for
Transformative Technologies;

Talk – Action = Zero

Conclusions

- We need to change the paradigm away from a zero-sum to a positive-sum model, where both privacy and security are built directly into technologies;
- The use of privacy-enhancing biometrics such as Biometric Encryption will ensure that privacy is protected, while at the same time, delivering strong security – a true win/win scenario – positive-sum, all the way!
- "Radical pragmatism" reflects an effort to embed privacy protective measures, such as privacy by design, into existing technologies and practices, in a positive-sum paradigm;
- Help us change the paradigm and think differently: Make it privacy AND security, not "either/or."

How to Contact Us

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca