Replace Zero-Sum with Positive-Sum to Deliver both Security and Privacy

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario

Ken Anderson
Assistant Information and Privacy Commissioner

McMaster University
May 14, 2008

Presentation Outline

1. *Privacy “101 – Setting the Stage*
2. *Privacy by Design*
3. *Transformative Technologies*
4. *Technology-Related Applications*
5. *Identity Management*
6. *Biometric Encryption*
7. *The Future, Right Now*

Privacy "101"
Setting the Stage

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."

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)

The Golden Rules:
Fair Information Practices

- **Why are you asking?**
  - Collection; purpose specification;
- **How will the information be used?**
  - Primary purpose; use limitation;
- **Any additional secondary uses?**
  - Notice and consent; prohibition against unauthorized disclosure;
- **Who will be able to see my information?**
  - Restricted access from unauthorized third parties.

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);
- United States Safe Harbor Agreement (2000);
- Global Privacy Standard (2006).

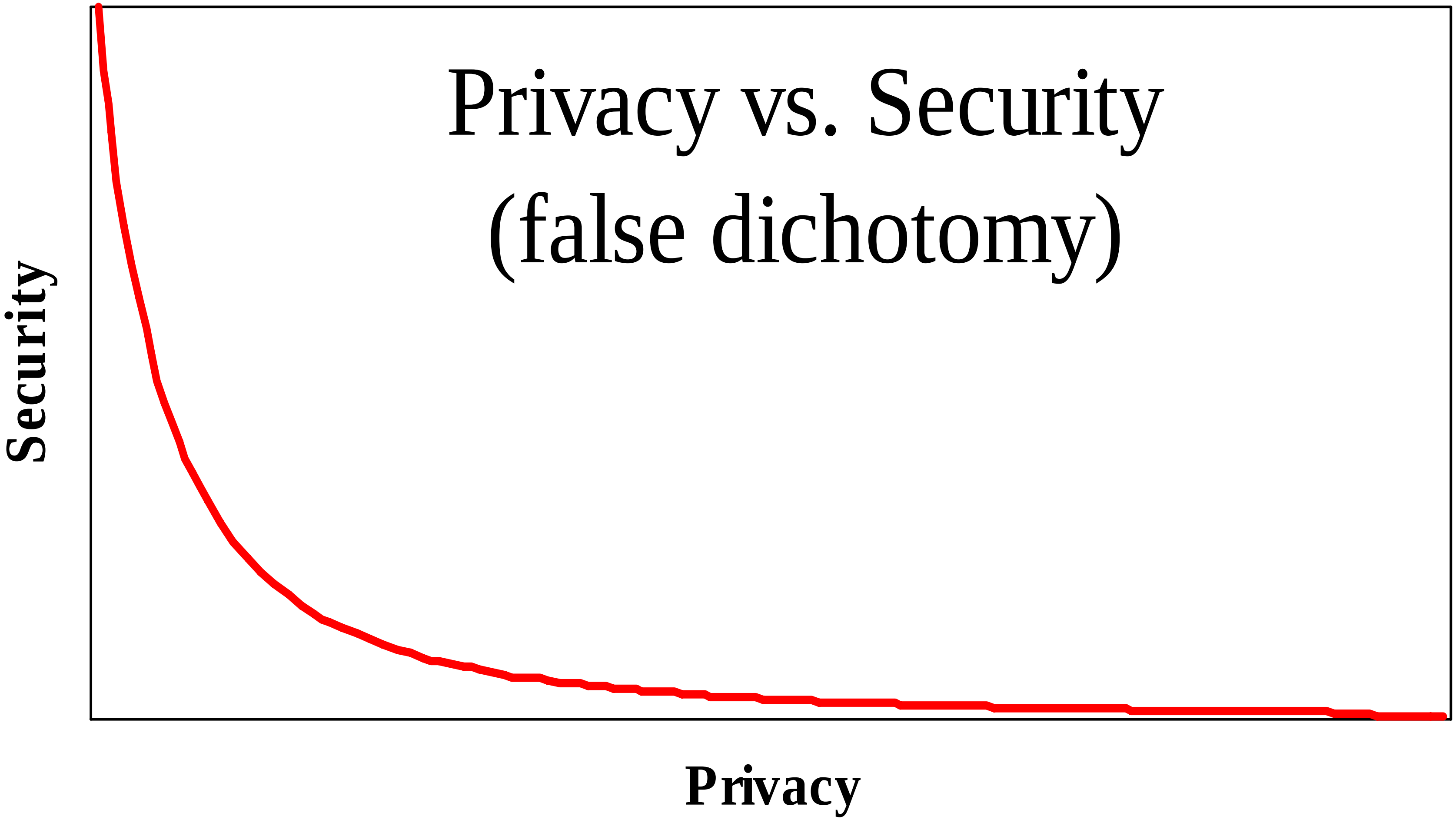
Global Privacy Standard

- 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 in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

www.ipc.on.ca/images/Resources/up-gps.pdf

Privacy vs. Security?
No

Privacy OR Security:
A Zero-Sum Game



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 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.

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).*

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.

2006
PET Workshop Award
for outstanding research
in the field of
Privacy Enhancing Technology
A Taxonomy of Privacy
Daniel J. Solove

Transformative Technologies

Surveillance Technology + Positive-Sum Thinking + Privacy Enhancing Technology =

Transformative Technologies

Common characteristics of Transformative Technologies:

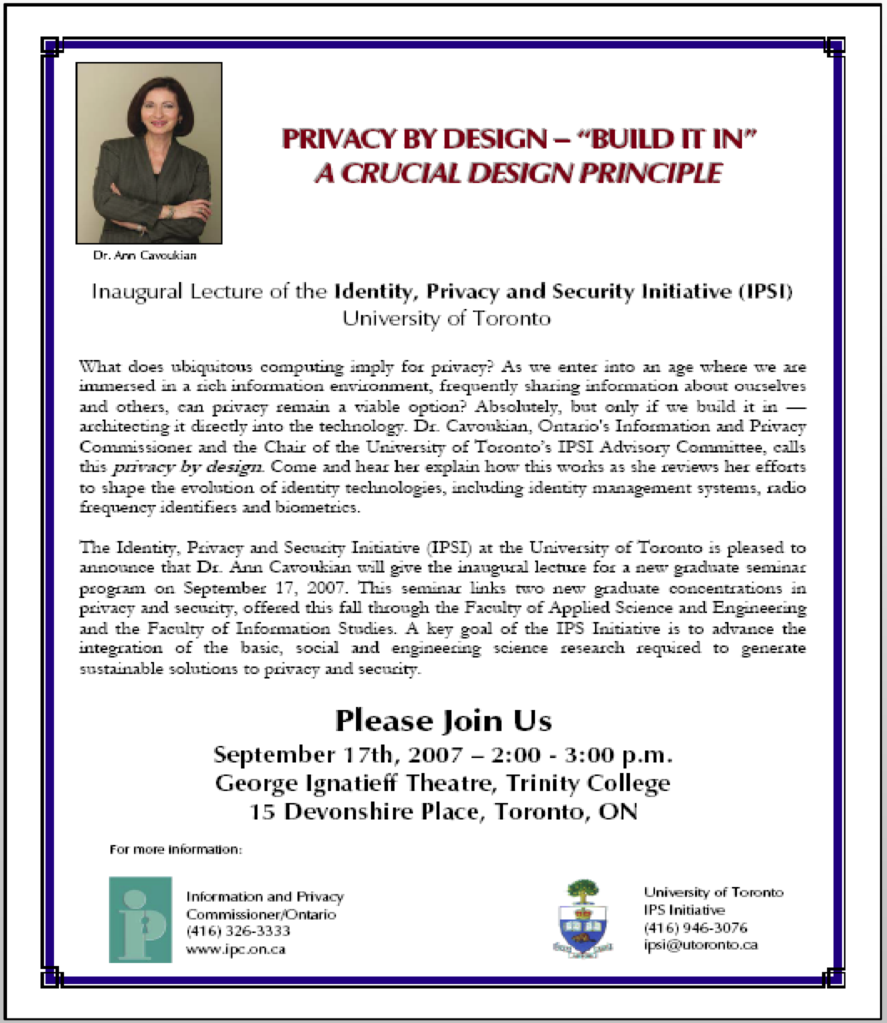
- Help minimize unnecessary disclosure, collection, retention and use of personal data;
- Empower individuals to participate in the management of their personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in (personal) data governance structures;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

IPSI

Identity, Privacy and Security Initiative

- As we enter into an age where we are immersed in a rich information environment, frequently sharing information about ourselves and others, can privacy remain a viable option?

- Absolutely, but only if we build it in — architecting it directly into the technology.



PRIVACY BY DESIGN – "BUILD IT IN"
A CRUCIAL DESIGN PRINCIPLE

Dr. Ann Cavoukian

Inaugural Lecture of the **Identity, Privacy and Security Initiative (IPSI)**
University of Toronto

What does ubiquitous computing imply for privacy? As we enter into an age where we are immersed in a rich information environment, frequently sharing information about ourselves and others, can privacy remain a viable option? Absolutely, but only if we build it in — architecting it directly into the technology. Dr. Cavoukian, Ontario's Information and Privacy Commissioner and the Chair of the University of Toronto's IPSI Advisory Committee, calls this *privacy by design*. Come and hear her explain how this works as she reviews her efforts to shape the evolution of identity technologies, including identity management systems, radio frequency identifiers and biometrics.

The Identity, Privacy and Security Initiative (IPSI) at the University of Toronto is pleased to announce that Dr. Ann Cavoukian will give the inaugural lecture for a new graduate seminar program on September 17, 2007. This seminar links two new graduate concentrations in privacy and security, offered this fall through the Faculty of Applied Science and Engineering and the Faculty of Information Studies. A key goal of the IPS Initiative is to advance the integration of the basic, social and engineering science research required to generate sustainable solutions to privacy and security.

Please Join Us

September 17th, 2007 – 2:00 - 3:00 p.m.
George Ignatieff Theatre, Trinity College
15 Devonshire Place, Toronto, ON

For more information:

Information and Privacy
Commissioner/Ontario
(416) 326-3333
www.ipc.on.ca

University of Toronto
IPS Initiative
(416) 946-3076
ipsi@utoronto.ca

www.ipsi.utoronto.ca/site4.aspx

Technology and Privacy-Related Applications

Ken Anderson

Technology and Privacy-Related Applications

- Identity Management;
- Biometric Encryption;

Identity Management

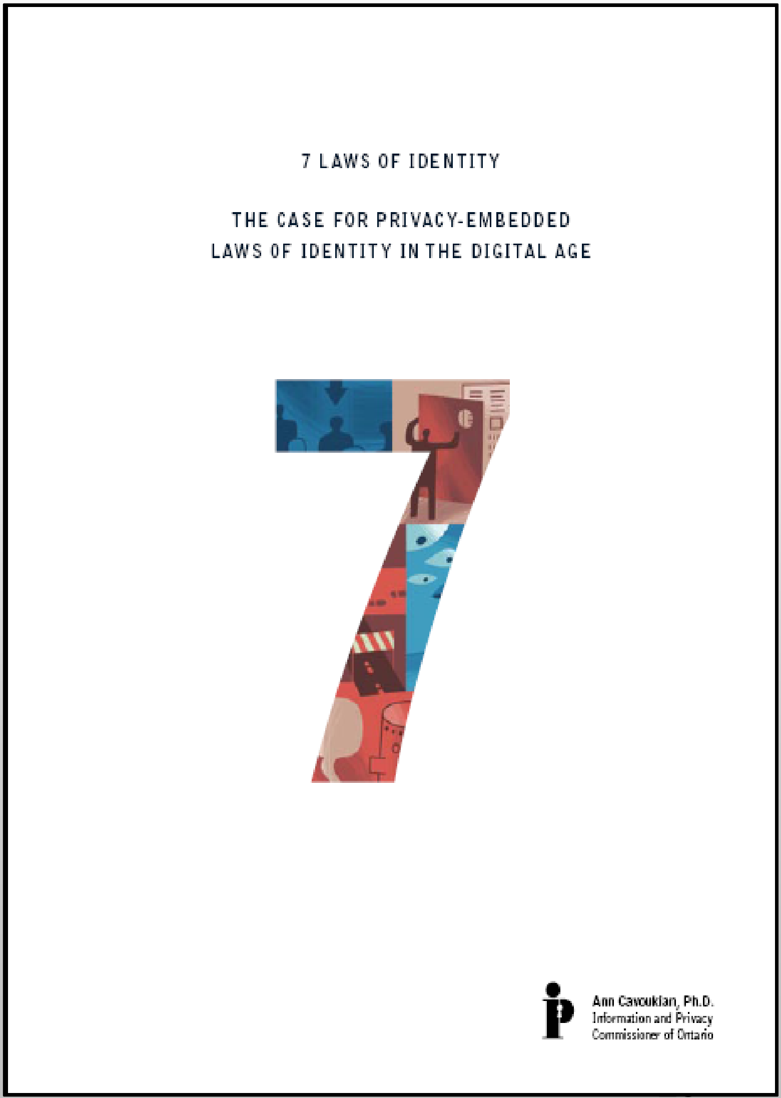
A Single Identity Metasystem

- Before the Internet, there were many different networks that did not speak the same language;
- With the introduction of TCP/IP, thousands of network externalities bloomed, and the Internet exploded;
- A similar phenomenon is being predicted today: a “TCP/IP” for linking different identity systems will open up endless new e-commerce possibilities ***– enter the Identity Metasystem, based on the 7 Laws of Identity.***

7 Privacy-Embedded Laws

The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities are so diminished as to lead to its demise. Enter the 7 Laws of Identity.

— Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario



7 LAWS OF IDENTITY

THE CASE FOR PRIVACY-EMBEDDED
LAWS OF IDENTITY IN THE DIGITAL AGE

Ann Cavoukian, Ph.D.
Information and Privacy
Commissioner of Ontario

www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf

Privacy in the Clouds

Evolution of Consumer Computing:

1. **The stand-alone PC** in which the user’s software and data are stored on a single, easily protected machine, such as word processing, spreadsheets;

2. **The Web** in which most of the software a user needs is still on their own PC, but more and more of the data they need is found on the Internet, such as a Web browser;

3. **The “Cloud”** in which users rely heavily on data and software that reside on the Internet. Examples: using Google Apps for word-processing; virtual worlds such as Second Life that enable users to build 3D environments combining Web pages and Web applications.

See *The Information Factories* by George Gilder, Wired magazine, October, 2006, www.wired.com/wired/archive/14.10/cloudware_pr.html

Biometric Encryption

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*.

www.e-laws.gov.on.ca/DBLaws/Statutes/English/97o25a_e.htm

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.

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

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)

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

Biometric Encryption (BE)

What is Biometric Encryption?

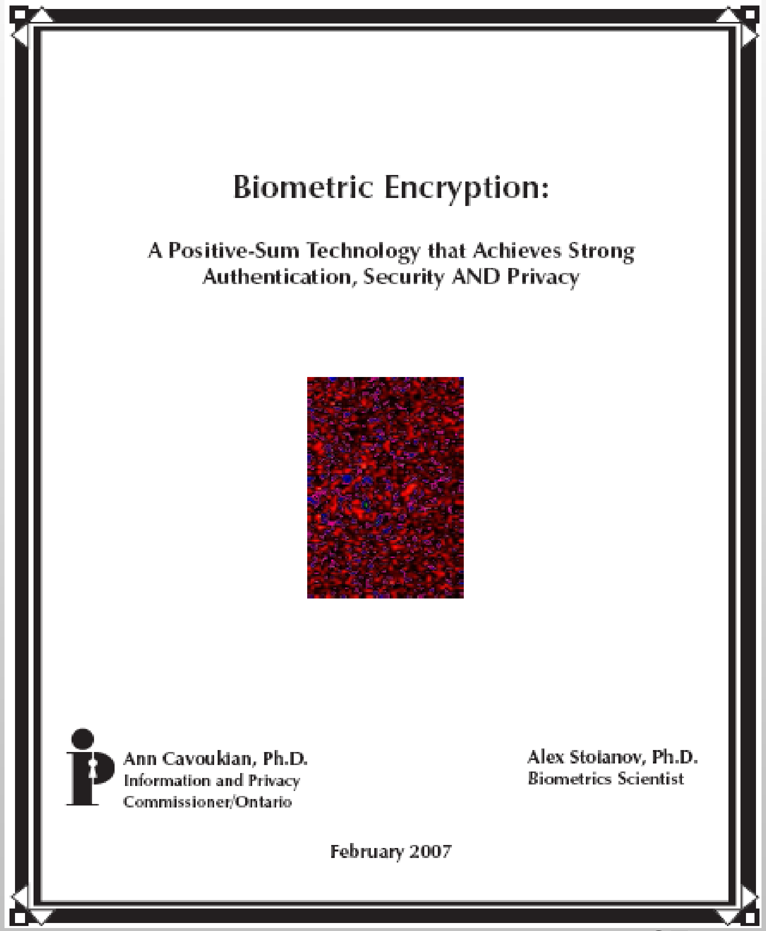
- Class of emerging “untraceable biometric” technologies that seek to transform the biometric data provided by the user;

- Special properties:
  - uniqueness
  - irreversibility

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 (i.e., that adding privacy to identification and information systems will necessarily weaken security and functionality).



Biometric Encryption:

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

Ann Cavoukian, Ph.D.
Information and Privacy
Commissioner/Ontario

Alex Stoianov, Ph.D.
Biometrics Scientist

February 2007

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

Advantages of Biometric Encryption

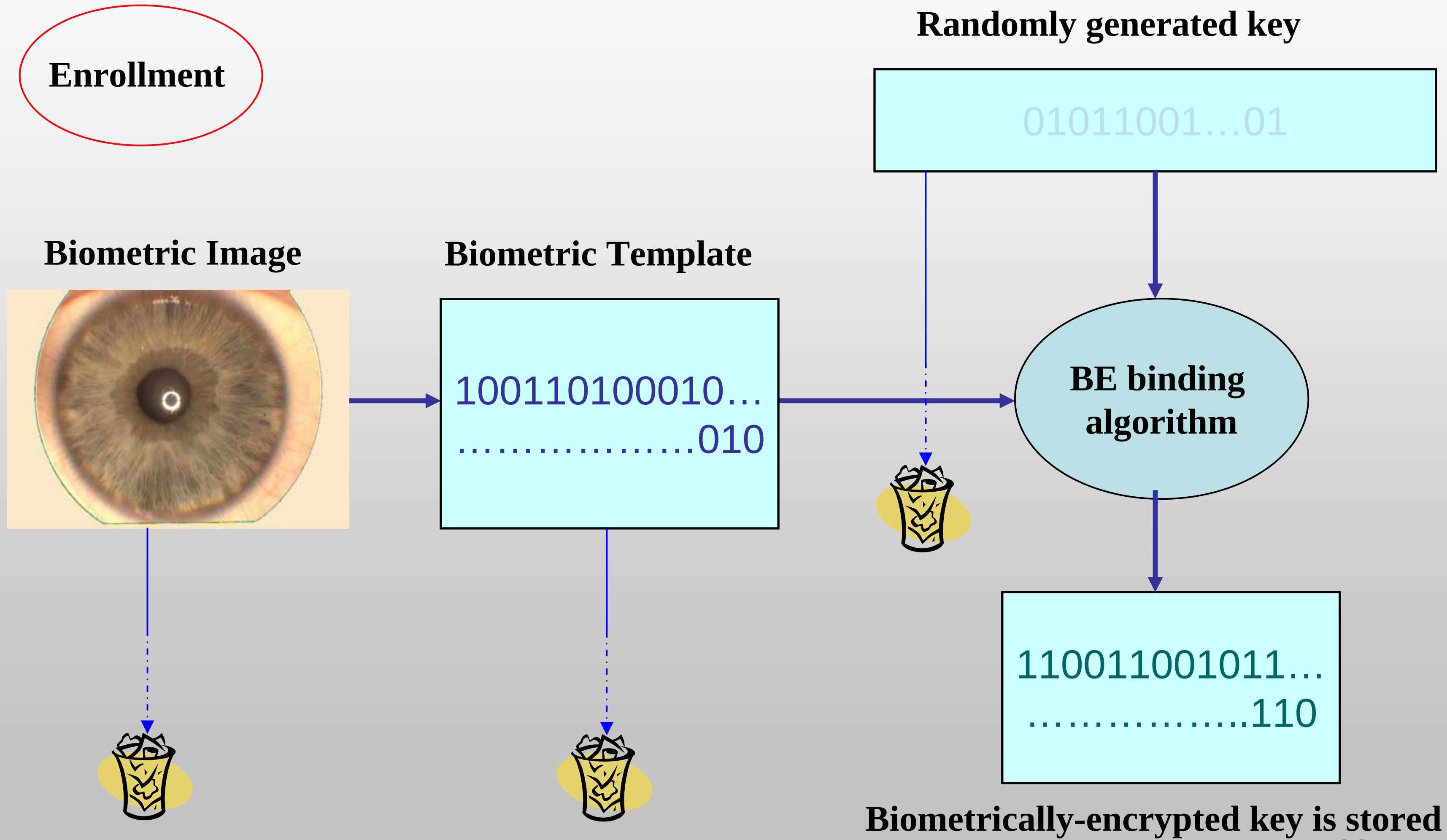
BE Embodies core privacy practices:

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



Enrollment

Randomly generated key

01011001…01

Biometric Image

Biometric Template

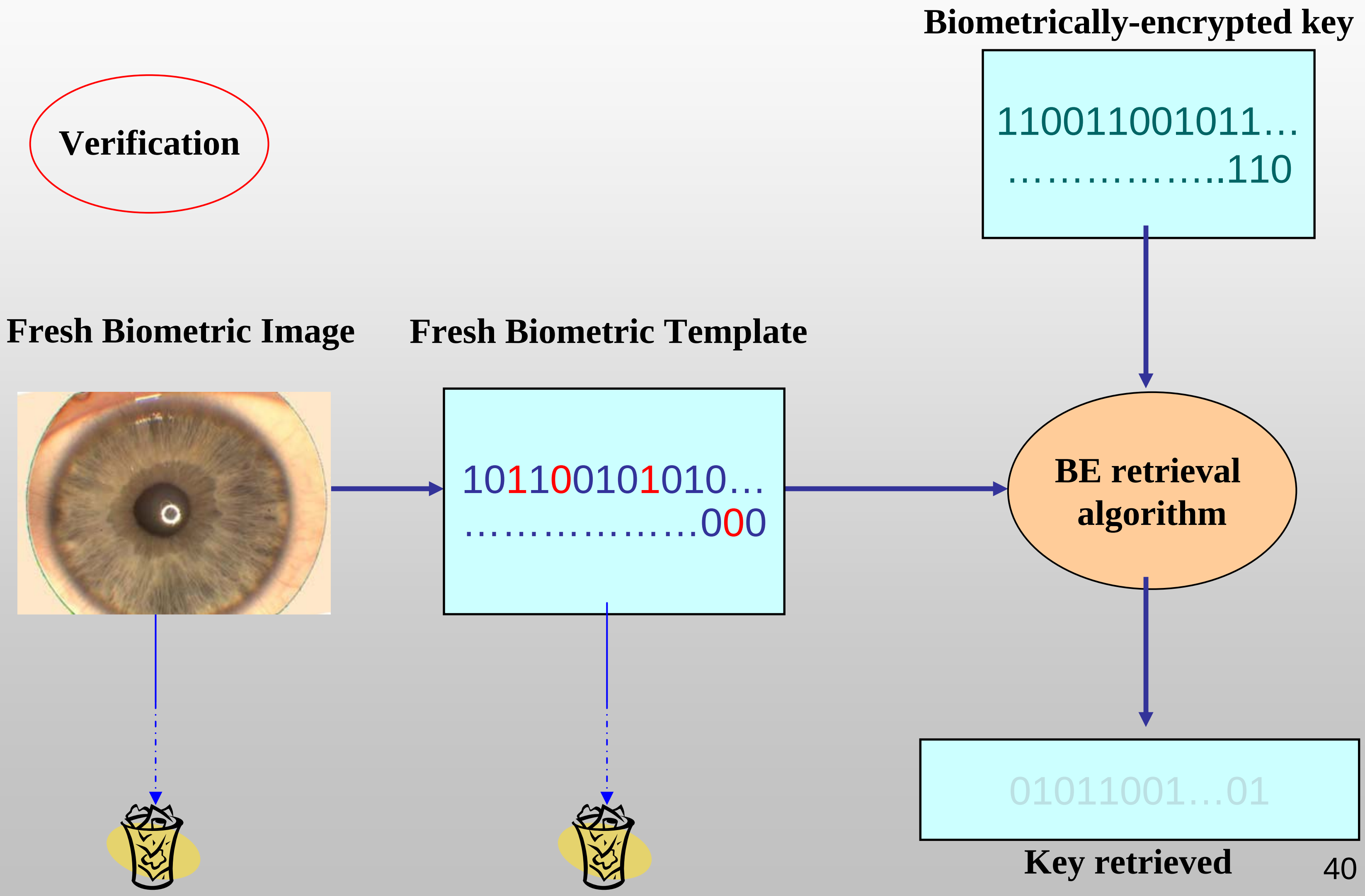
100110100010…
………………..010

BE binding algorithm

110011001011…
……………..110

Biometrically-encrypted key is stored

Decrypt with Same Biometric



Verification

Biometrically-encrypted key

110011001011…
………………110

Fresh Biometric Image

Fresh Biometric Template

1011100101010…
………………..000

BE retrieval algorithm

01011001…01

Key retrieved

BE Technologies

- Fuzzy Commitment/Fuzzy Extractor scheme:
  - Philips privID^{TM} : 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.

Attacks on Biometric Encryption

- Bioscrypt BE: may be vulnerable to hill climbing attack;
- Fuzzy Vault: may be vulnerable to re-usability attack, hill climbing attack (?);
- Daugman's iris scheme: may be vulnerable to attack on ECC;
- Philips privID: seems to be robust to all attacks;

- A cryptographic yardstick should not be applied to BE;
- Two-tier authentication: password/token integrated with BE.

Common Technical Question:

Q: You say that there is a BE template, also called a "private template" or "helper data". Is there an intermediate "key encrypting key" or other defined subset of information, stored in the BE template?

A: No, there is no intermediate "key encrypting key" or other defined subset of information, with BE. Redundancy in the biometric is used to consistently decrypt the key.

Common Technical Question:

Q: There are other products on the market claiming that they use “biometric encryption” or some similar terminology. How are they different from the BE discussed in the paper?

A: We used the term Biometric Encryption (BE) in a broad sense to include all the technologies that bind a key to a biometric or generate a key from a biometric (the latter are practically nonexistent)…

Common Technical Question:

Q: What is the difference between BE and Cancellable Biometrics (CB)?

A: Similarities between BE and CB:

a) the biometric image/template is transformed to a domain from which it cannot be recovered;

b) the transformation is application dependent;

c) the resulting BE or CB template is cancelable (revocable).

A: Differences:

a) in BE, a key is bound to the biometric and is released on verification.
The output is either a key or a failure message.

b) In CB, the output is a binary Yes/No response.

Current IPC 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;
- **Bell Canada** is deploying a voluntary voice identity verification service for its customers using technology by biometric vendor **PerSay** (Israel); after only 2 months, Philips was able to clearly demonstrate with success the feasibility of integrating their BE technology with PerSay's voice technology;
- The **Ontario Lottery and Gaming Corporation** (OLG) is exploring the use of facial biometrics to assist Ontarians who voluntarily choose, under the self-exclusion program, to provide photos of themselves so that they can be denied entry into casinos because of their gambling addiction.

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**