Change the Paradigm:
Transformative Technologies for Privacy

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

October 23, 2008
Research and Innovation for Security, Privacy and Trustworthiness in the Information Society
Athens, Greece

Privacy = Freedom

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."

Global Privacy Standard

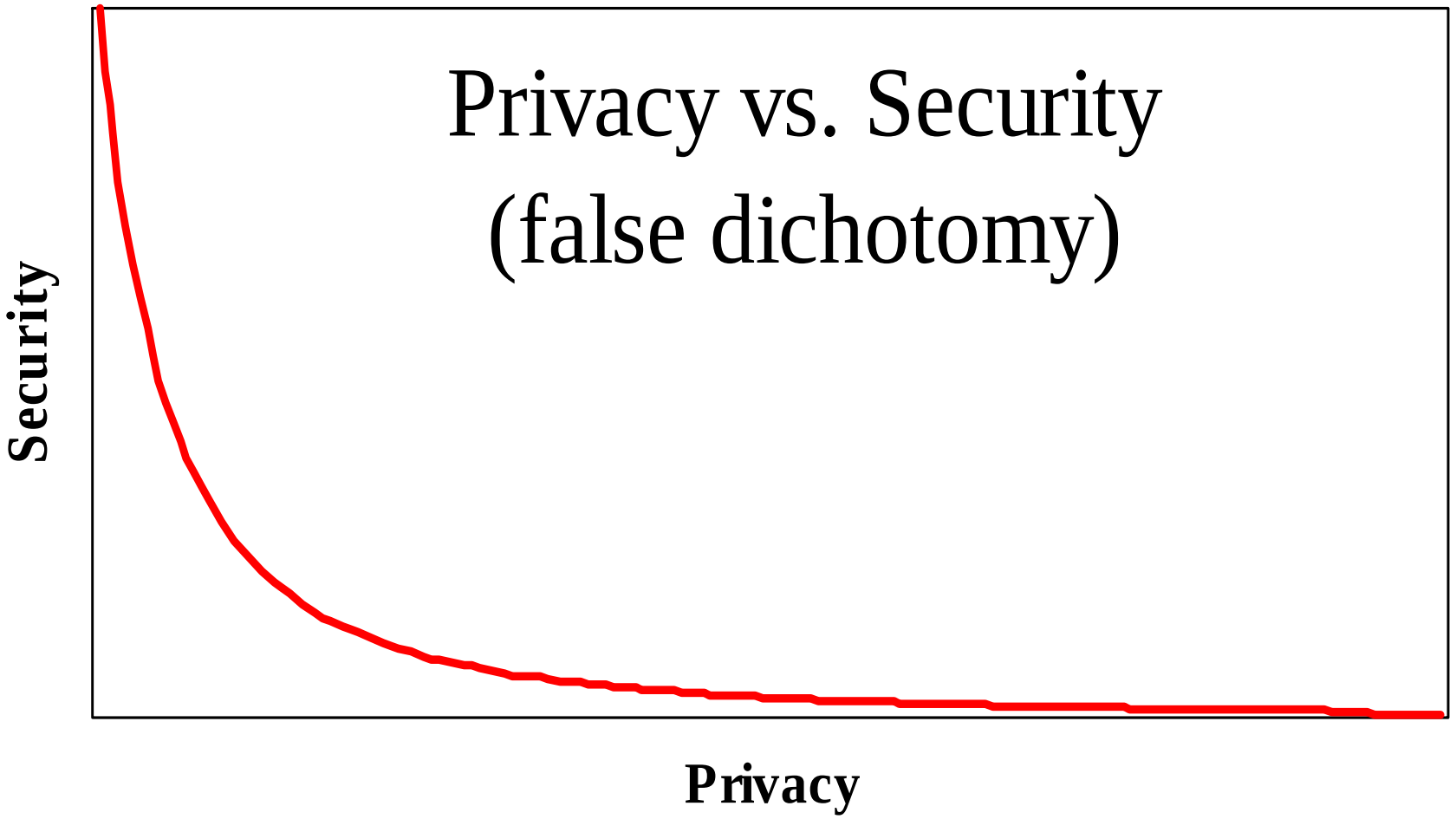
- In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners convened for the sole purpose of creating a single Global Privacy Standard (GPS);
- Globalization and converging business practices created a need to harmonize 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

If Privacy is to Survive, Things Have to Change

Positive-Sum
NOT
Zero-Sum

Privacy OR Security:
A Zero-Sum Game



We Need to

Change

The Paradigm

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 often comes at the expense of privacy – the more you have of one, the less you have of the other;
- A **Positive-Sum Paradigm**, in contrast, 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 a minimization of 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: "Build It In"

- I first developed the term "Privacy by Design" in the 1990's, as a response to the growing threats to online privacy that were beginning to emerge;
- "Privacy by Design" seeks to build in privacy – up front, into the design specifications; into the architecture; 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) where possible: give people maximum control over their own data.

Privacy-Enhancing Technologies *(PETs)*

- The IPC developed 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).***

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

From PETs to Trans Tech

The Next Wave: Transformative Technologies

Transformative Technologies *(PETs Plus)*

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

<u>Transformative Technology</u>

Common characteristics of Transformative Technologies:

- Minimize the unnecessary collection, disclosure, use and retention of personal data;
- Empower individuals to participate in the management of their own personal data;
- Enhance the security of personal data, if collected/used;
- Promote public confidence and trust in personal data governance structures;
- Promote/facilitate the commercialization and adoption of these technologies.

Biometrics Transformed: Biometric Encryption

IPC and Biometrics

- The IPC has been a longstanding proponent of biometric encryption technologies;
- We continue to press for strong privacy protections in the development and deployment of interoperable biometric technologies;
- Active member of the European Biometrics Forum International Biometrics Advisory Council (IBAC).

www.eubiometricforum.com/index.php?option=content&task=view&id=457

European Biometrics Forum

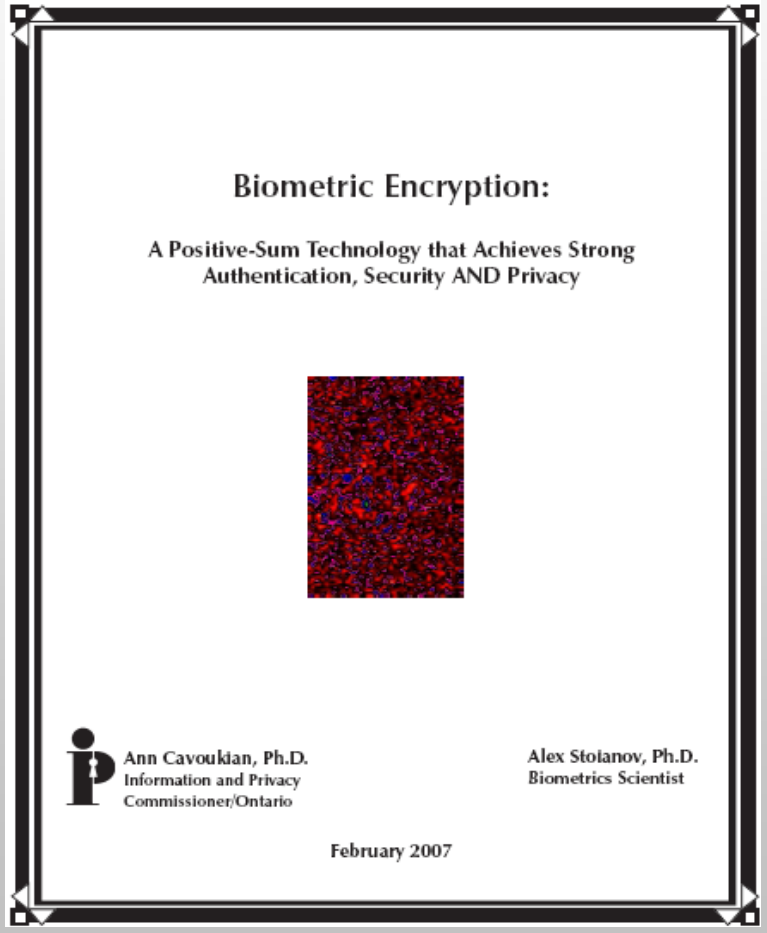
- The European Biometrics Forum (EBF) was launched in 2003; Member of International Biometrics Advisory Council (IBAC);
- Composed of leading biometrics and technology experts, the EBF was established to develop world-class standards, best practices and innovation in the biometrics industry to strengthen 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 to 2010.

www.eubiometricforum.com

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

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.

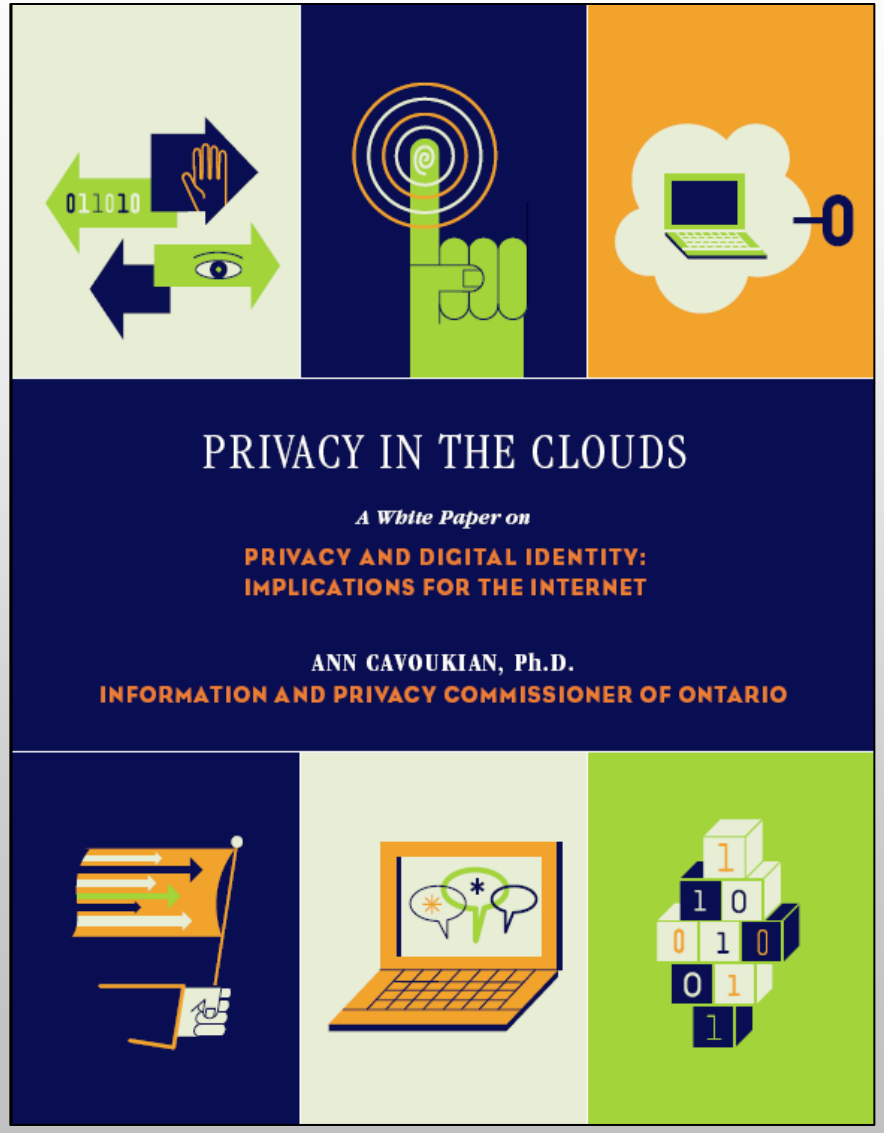
Biometric Encryption

- Biometric encryption is a process that securely binds a PIN or a cryptographic key with a biometric, so that neither the key nor the biometric can be retrieved. The key is recreated only if the correct live biometric sample (a finger or iris) is presented on verification;
- In biometric encryption, you can use the biometric to encrypt a PIN or a password for numerous applications, such as access to computers or bank machines. The PIN can be 100s of digits in length since you don't need to remember it;
- Most important, the only item that has to be stored in a database is the biometrically encrypted PIN or password, not the biometric template, so privacy is preserved.

Privacy in the Clouds

Clouds Building Blocks:

1. Open source and proprietary identity software based on open standards;
2. Federated identity;
3. Multiple and partial identities;
4. Data-centred policies;
5. Audit tools;



www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

Conclusions

- We need to change the paradigm away from a zero-sum game 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;
- Work with us to change the paradigm and think differently: We need both 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