



Privacy by Design in Biometrics: *Think Positive-Sum, not Zero-sum*

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

Northwind Professional Institute
Privacy Invitational Forum
November 6, 2008



Presentation Outline

1. *“Privacy by Design”*
2. *Positive-Sum, Not Zero-Sum*
3. *The Next Wave: (PETs Plus),
Transformative Technologies*
4. *Biometrics and Privacy*
5. *Conclusions*



“Privacy by Design”



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*)

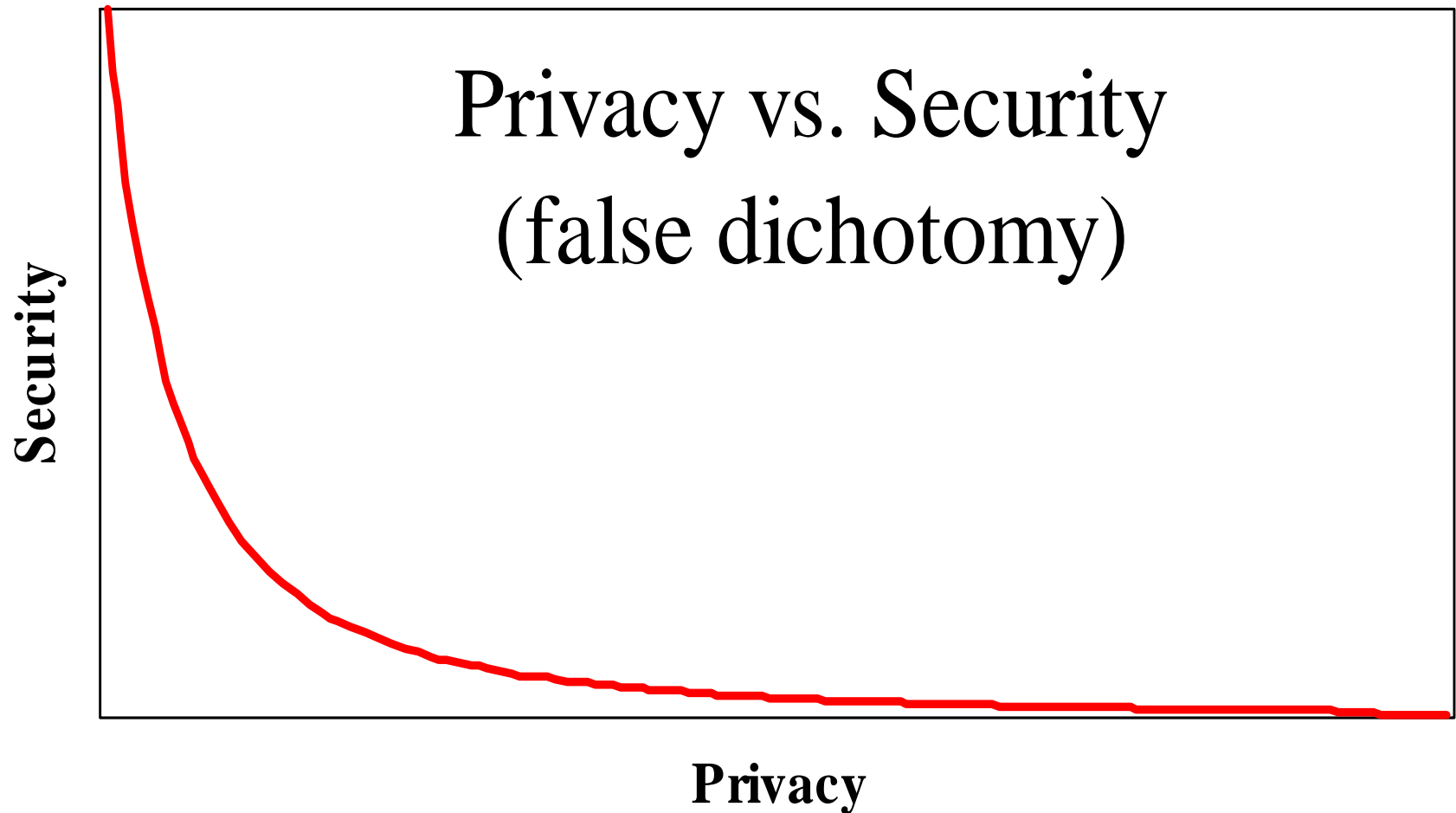
- Privacy Enhancing Technologies enlist the support of technology to **protect** privacy. They include those that empower individuals to manage their own identities and personally-identifiable information (PII) in a privacy enhancing manner – encryption plays a key role.
- These include tools or systems 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.



Positive-Sum
NOT
Zero-Sum



Privacy OR Security: *A Zero-Sum Game*





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*



*The Next Wave:
“Transformative Technologies”
(PETs Plus)*



Time For A Change...

*... from PETs to PETs Plus,
or Transformative Technologies*



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.



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.



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

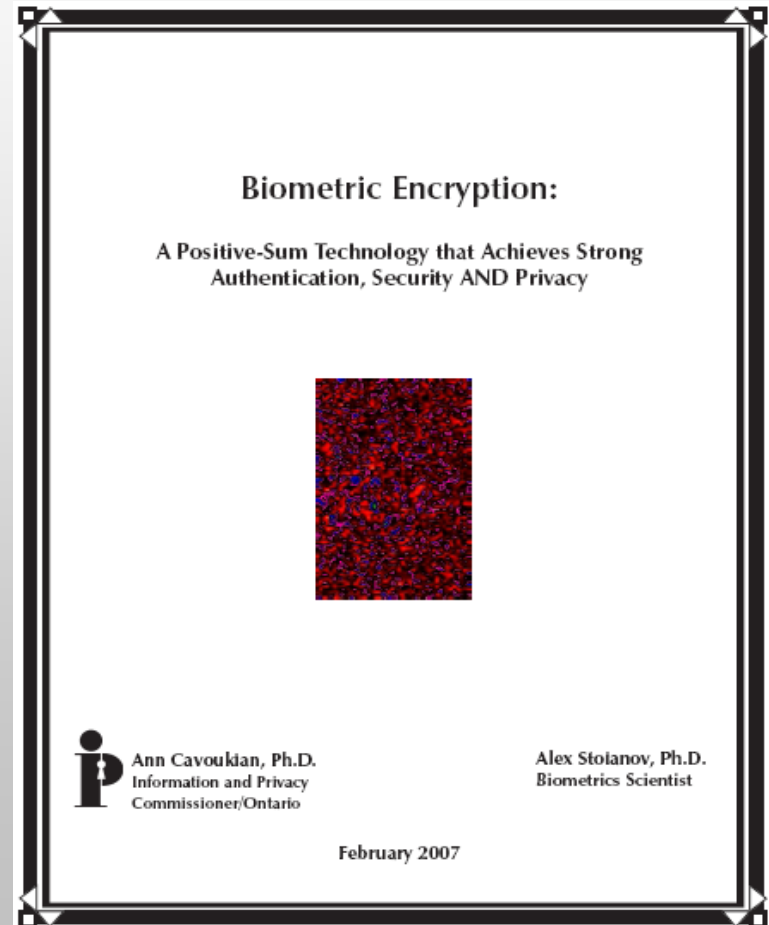
* Pioneering development by George Tomko, Ph.D.
Founder of Mytec Technologies, 1994.



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.





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.



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.



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!
- We need to change the paradigm to enable both privacy AND security, not “either/or,” entailing unnecessary trade-offs.



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