“Privacy by Design”

A Crucial Design Principle

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

University of Waterloo

February 27, 2007

Presentation Outline

1. *Privacy 101*
2. *What is Privacy?*
3. *Fair Information Practices*
4. *Privacy Enhancing Technologies*
5. *Identity Management: The Need for An Over-Arching Plan*
6. *Privacy-Embedded 7 Laws*
7. *Conclusion*

Privacy 101

IPC: Responsibilities

Under its statutory mandate, the Commissioner 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.

Commissioner's Powers

The Commissioner is appointed by the Ontario legislature and is independent from the government;

The Commissioner has the power to:

- Offer comment on the privacy protection implications of proposed programs of institutions;
- In appropriate circumstances, authorize the collection of personal information otherwise than directly from the individual;
- Engage in or commission research into matters affecting the carrying out of the purposes of the *Acts*;
- Conduct public education programs and provide information concerning this Act and the Commissioner's role and activities;
- Receive representations from the public concerning the operation of the *Acts;*
- Order the disclosure of government-held information.

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;
  - Fair Information Practices.

IPC

Personally Identifiable Information

Under Ontario’s privacy legislation, “personal information" means recorded information about an identifiable individual:

- Name;
- Address;
- Sex, Age;
- Education;
- Employment history;
- Financial information;
- And any other information about the individual.

- Health information is a special case, falling under the *Personal Health Information Protection Act.*

What Privacy is Not

Privacy ≠ Security

Privacy and Security: *The Difference*

- Authentication
- Data Integrity
- Confidentiality
- Non-repudiation

Security:

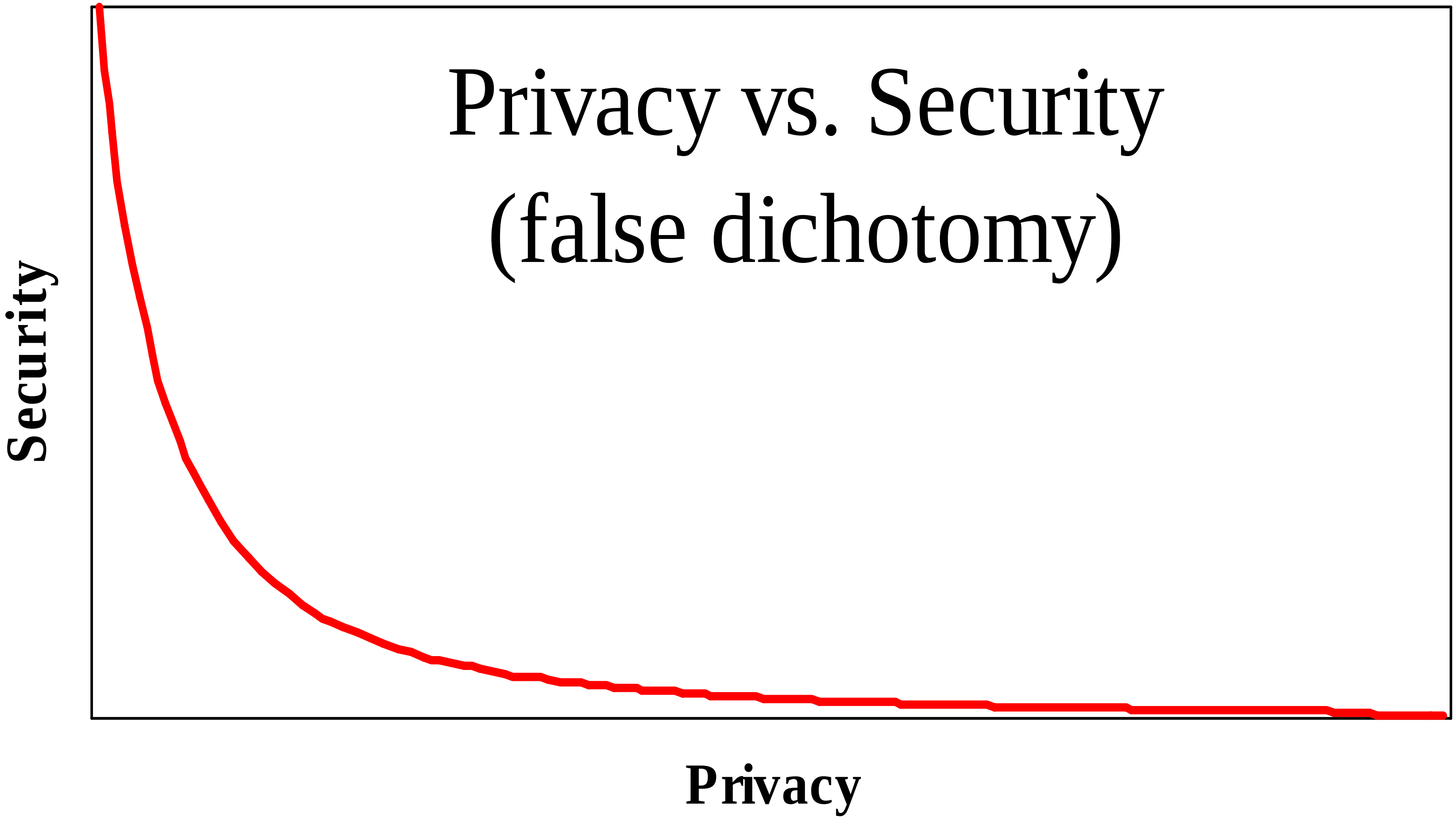
Organizational control of information through information systems

- Privacy; Data Protection
- Fair Information Practices

What We Don’t Want…

PRIVACY
CLOSED TEMPORARILY
SECURITY

Privacy OR Security:
A Zero-Sum Game



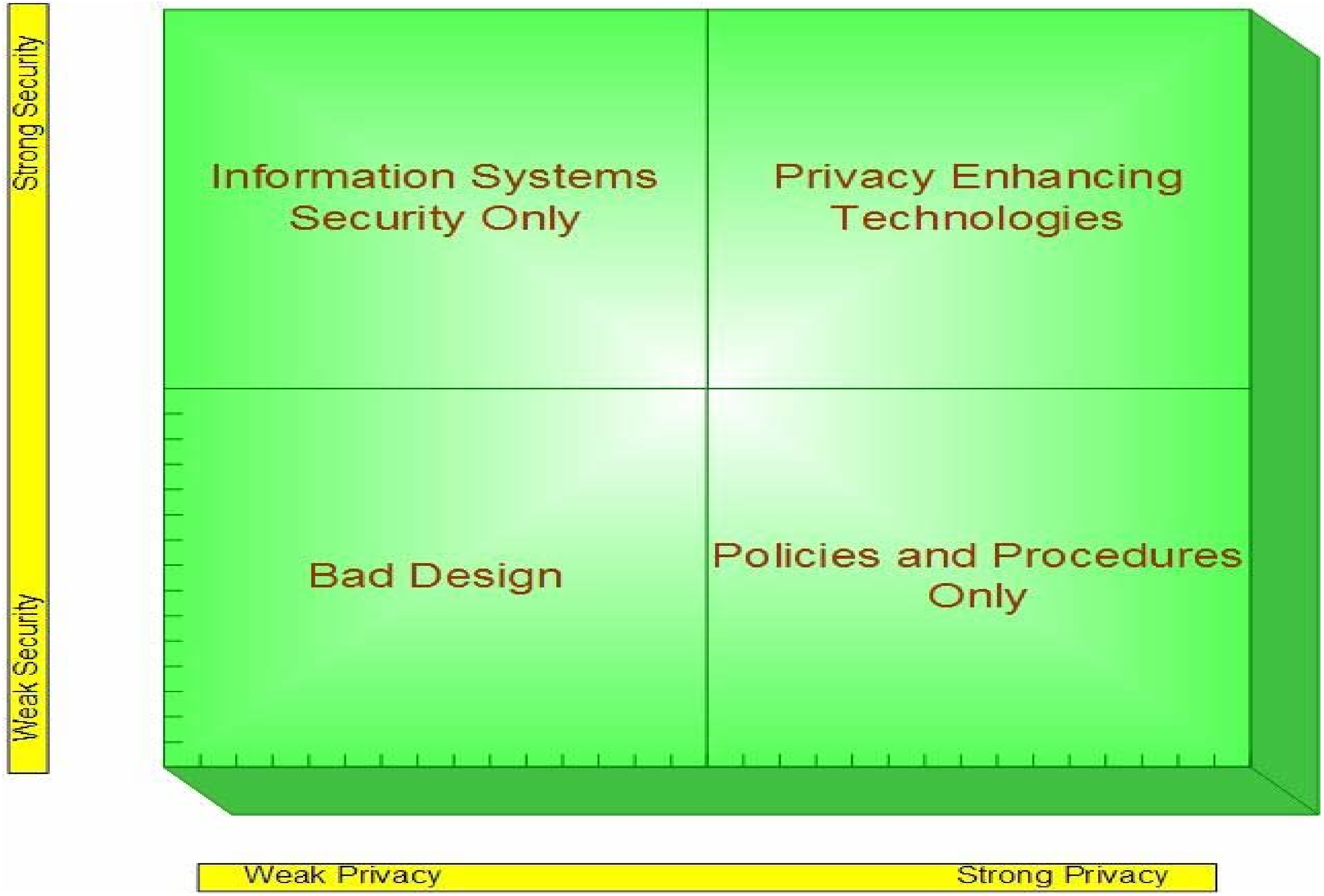
Privacy vs. Security
(false dichotomy)

Positive-Sum Model

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

IPC

Privacy AND Security



Information Systems Security Only

Privacy Enhancing Technologies

Bad Design

Policies and Procedures Only

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);
- United States Safe Harbor Agreement (2000).

CSA Model Code

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

CSA's ***Model Code for the Protection of Personal Information***

Privacy Laws

Canada, the United States and Europe

Canada:

Public sector privacy laws: federal, provincial and municipal;
Private sector privacy laws: (Federal) *Personal Information Protection and Electronic Documents Act (PIPEDA)*;
Provincial: Quebec, British Columbia, Alberta, Ontario.

United States:

Federal public sector *Privacy Act;*
Sectoral privacy laws;
Safe Harbor Agreement;

Europe:

Both private and public sector privacy laws;
- European Directive on Data Protection.

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 Enhancing Technologies (PETs)

Why PETs?

- If asked, “Imagine that someone does not know you but knows your date of birth, sex, and zip code; What do you think the probability is that they could uniquely identify you based on this information?”
- In a survey at Carnegie-Mellon University, almost all answered, “less than 50%;”
- ***The reality is closer to 90%*** - Using 1990 census data, 87% of the U.S. population could be uniquely identified with the above data.

- Sweeny, *Uniqueness of Simple Demographics in the U.S. Population.*
http://privacy.cs.cmu.edu

Benefits of PETs

- Data protection, such as encryption, is markedly less expensive than cleaning up after a data breach;
- Research has shown that it would cost about $6 per customer account to encrypt data;

  — Avivah Litan, Gartner Analyst
- The cost of a breach is much higher – ***30 times higher.*** In 2006, the average number of records compromised in a corporate privacy breach was about 25,000. At an average cost of $182 per record, this meant that each privacy breach incident cost $4.7 million;

  — Ponemon Institute
- 100,000 records encrypted = $600,000 vs.
  100,000 records breached = $18,200,000
  — ***You do the math.***

IPC

www.ponemon.org/press/Ponemon_2006%20Data%20Breach%20Cost_FINAL.pdf

“U-Prove SDK”

Credentica Privacy Technology Product

- **Founder and CEO of Credentica, Dr. Stefan Brands** has developed this privacy-enhanced user-centric identity management tool that can be integrated with current identity management systems and is consistent with the 7 privacy-embedded Laws of Identity, notably:
  - Personal Control and Consent;
  - Minimal Disclosure for Limited Use: Data Minimization;
  - Justifiable Parties: Need to Know Access;
  - Directed Identity: Protection and Accountability, and;
  - Pluralism of Operators and Technologies: Minimizing Surveillance.
- This is a true Privacy Enhancing Technology (PET) which has been tested and vetted extensively by a dozen world-class cryptographers and leading companies.

www.credentica.com

Other Practical PETs

- Private Electronic Conversations;

  OTR (Off The Record) Messaging

- Trusted Small Platforms;

  Elliptical Curve Cryptography

- Pragmatic Commercial Privacy;

  The IBM RFID "Clipped" Tag

OTR Messaging

How do you replicate the privacy of a street conversation on the web? Called “Off The Record” Messaging, it incorporates:

- **Encryption**
- **Authentication**
- **Deniability**
- **Perfect forward secrecy**

www.cypherpunks.ca/otr/

Elliptical Curve Cryptography (ECC)

- Co-invented by Neal Koblitz and Victor S. Miller as an alternative way of doing public key cryptography;
- A distinct approach to either public key or asymmetric cryptography:
  - A set of algorithms for key generation, encryption and decryption;
- Keys in elliptic curve cryptography can be chosen to be much shorter for a comparable level of security, or more security per bit.

More Security Per Bit

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

NIST Recommended Key Sizes

IPC

RFID Privacy Challenges

- **Perceived Lack of Transparency, Consumer Trust:**

- RFID technology, current uses, still not well known or understood by the public. Public opinion on RFID still developing; highly volatile;

- Perceived as a privacy issue: public concerns about possible surveillance, secondary and unethical data uses;

- Lack of consumer voice, input; possibility of backlash;

- Need to be proactive, **take action now**.

Supply-Chain vs. Item-Level *The Difference*

- Every RFID tag contains unique-identifying data, such as a serial number;

- Privacy issues can arise when the RFID tag is associated with a specific item (rather than several items grouped together) ***and an identifiable individual (consumer);***

- **Supply-chain management**: involves tagging bulk goods, cases, pallets. Also some individual products for business uses in manufacturing, wholesale distribution, and for back-end retail inventory management purposes;

- **Item-level consumer product tagging**: involves tagging commercial products in the retail space that are owned, carried and used by individual consumers, such as apparel, electronics, and identity or payment cards.

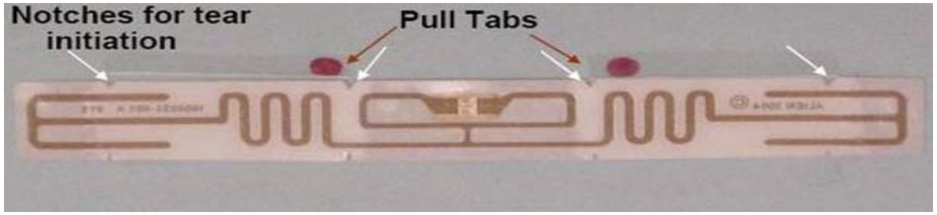
One Privacy Solution: *De-activation*

- Item-level RFID tags used in the retail sector should be deactivated at the point of sale;
- Deactivation at point of sale should be the default, but it is not without its problems;
- Deactivation limits post-sale benefits of RFIDs.

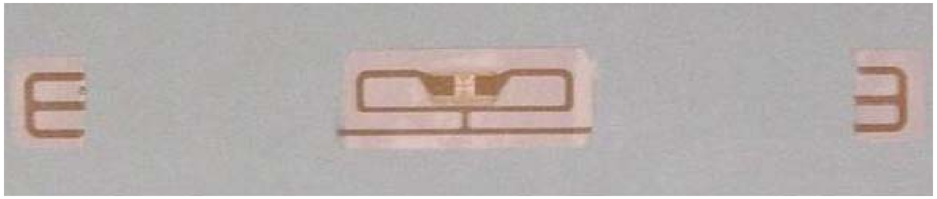
Practical Privacy:
IBM's "Clipped" Tag

- Provide RFID tag structures that permit a consumer to disable a tag by mechanically altering the tag in such a way as to inhibit the ability of a reader to interrogate the tag or transponder by wireless means:
  - Provides visual confirmation that tag has been deactivated (disabled);
  - May be read later on by mechanical contact if desired by consumer.

Before



After



Identity Management: The Need for an Over-Arching Plan

IPC

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.***

The Genius of the Identity Metasystem

- Developed by Microsoft’s Chief Identity Architect, Kim Cameron, the 7 Laws of Identity are technologically-necessary principles of identity management;
- The 7 Laws describe an identity metasystem for allowing different identity systems to function simultaneously;
- The genius of the identity metasystem is that it seeks to allow interoperability, with minimal disruption or modification to current ID systems.

The Big Bang

Supporters of the 7 Laws and the Identity Metasystem call this the “Identity Big Bang” that will enable ubiquitous intelligent services and a true marketplace for portable identities ***(Web 2.0).***

Privacy-Embedded

Laws

How the IPC Came to Work with Microsoft

- Introduced to the idea of the 7 Laws of Identity and the Identity Metasystem by Kim Cameron, Microsoft's Chief Identity Architect, who directed this endeavor with a diverse group of experts;
- As Commissioner, I wanted to *attempt* to influence the future direction of the 7 Laws, in the direction of privacy. In order to do that, the language of privacy had to be added and figure prominently in the Laws.

IPC's "Privacy-Embedded" 7 Laws of Identity

- An identity metasystem (described by the 7 Laws) is a necessary but not sufficient condition for privacy-enhancing options to be developed;
- What was needed was privacy-enabling design options for identity systems to be identified and then embedded, thus immersing privacy and data protection into the design;
- The privacy-embedded Identity Metasystem is the result of "mapping" fair information practices over the 7 Laws, to explicitly extract their privacy-protective features;
- The result is a commentary on the 7 Laws that extracts its privacy implications, for all to consider.

“Privacy-Embedded” 7 Laws of Identity

1. **Personal Control and Consent:**

   Technical identity systems must only reveal information identifying a user with the user’s consent;

2. **Minimal Disclosure For Limited Use: Data Minimization**
   The Identity Metasystem must disclose the least identifying information possible. This is the most stable, long-term solution. It is also the most privacy protective solution;

3. **Justifiable Parties: “Need To Know” Access**

   Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship;

IPC

“Privacy-Embedded” 7 Laws of Identity (Cont’d)

4. **Directed Identity: Protection and Accountability**

   A universal Identity Metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy;

5. **Pluralism of Operators and Technologies: Minimizing Surveillance**

   The interoperability of different identity technologies and their providers must be enabled by a universal Identity Metasystem;

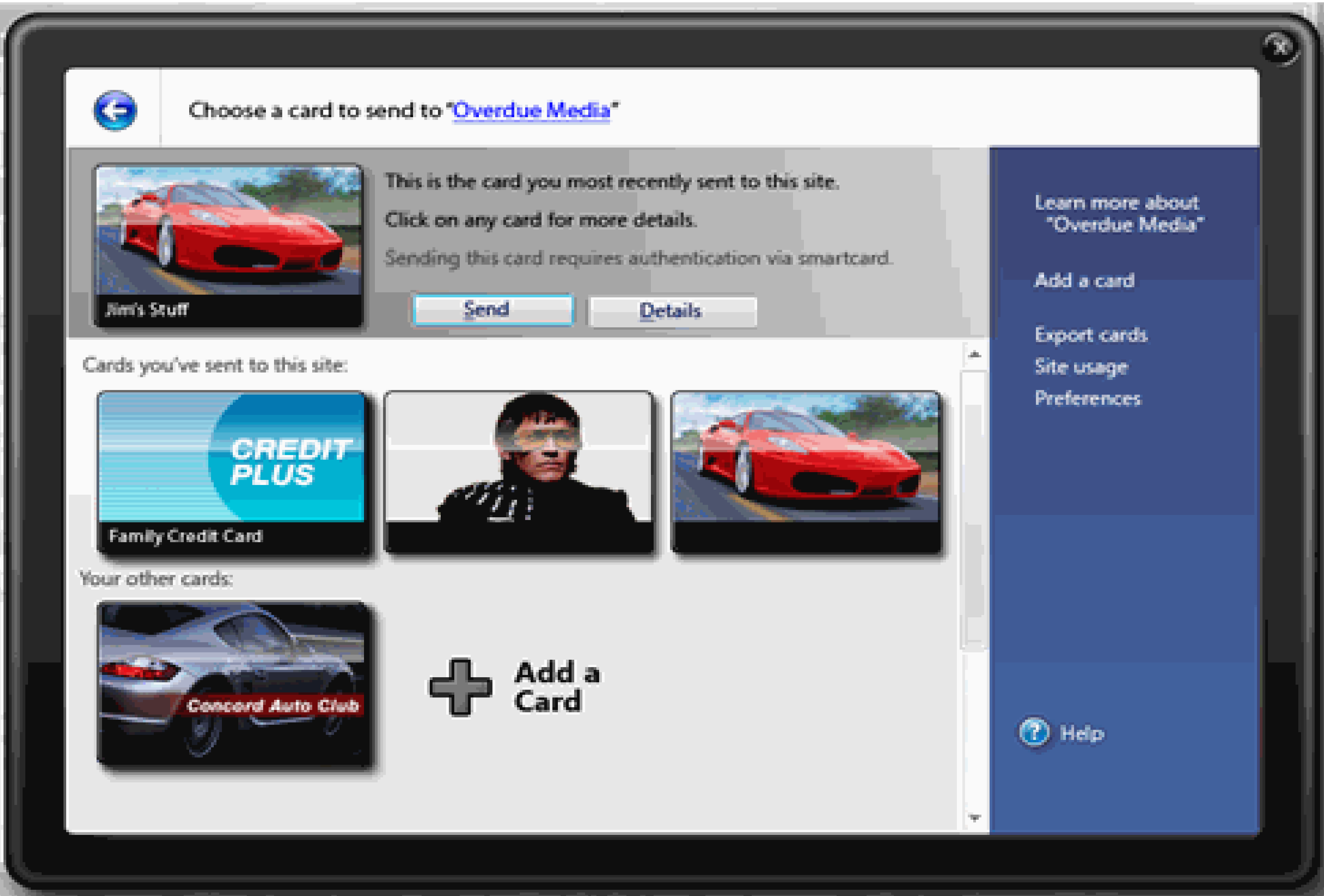
6. **The Human Face: Understanding Is Key**

   Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks;

7. **Consistent Experience Across Contexts: Enhanced User Empowerment And Control**

   The unifying Identity Metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Information Cards



Choose a card to send to "Overdue Media"

This is the card you most recently sent to this site.

Click on any card for more details.

Sending this card requires authentication via smartcard.

Cards you've sent to this site:

Your other cards:

Learn more about "Overdue Media"

Add a card

Export cards

Site usage

Preferences

Implications for Users

The Privacy-Embedded 7 Laws of Identity offer:

- Easier and more direct control over one's personal information when online;
- Embedded ability to minimize the amount of identifying data revealed online;
- Embedded ability to minimize the linkage between different identities and online activities;
- Embedded ability to detect fraudulent email messages and web sites (less phishing, pharming, online fraud).

IPC

IPC Consultation and Collaboration, on Internet Identity Issues

- October 2006, the IPC called upon software developers, the privacy community and public policy-makers to consider the Privacy-Embedded 7 Laws of Identity closely, to discuss them publicly, and to take them to heart;

- Many have taken us up, stepping forward to present their own ID management projects, and to explain how their solutions are user-centric, privacy-respecting and privacy-enhancing;

- The IPC is currently in discussions with several open-source identity management initiatives, such as with members of Liberty Alliance (Sun/Oracle) and Project Higgins (IBM), among others, to further advance individual privacy in the identity age;

- We will be publishing several discussion papers on identity with these parties – ***stay tuned!***

Biometrics White Paper

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.

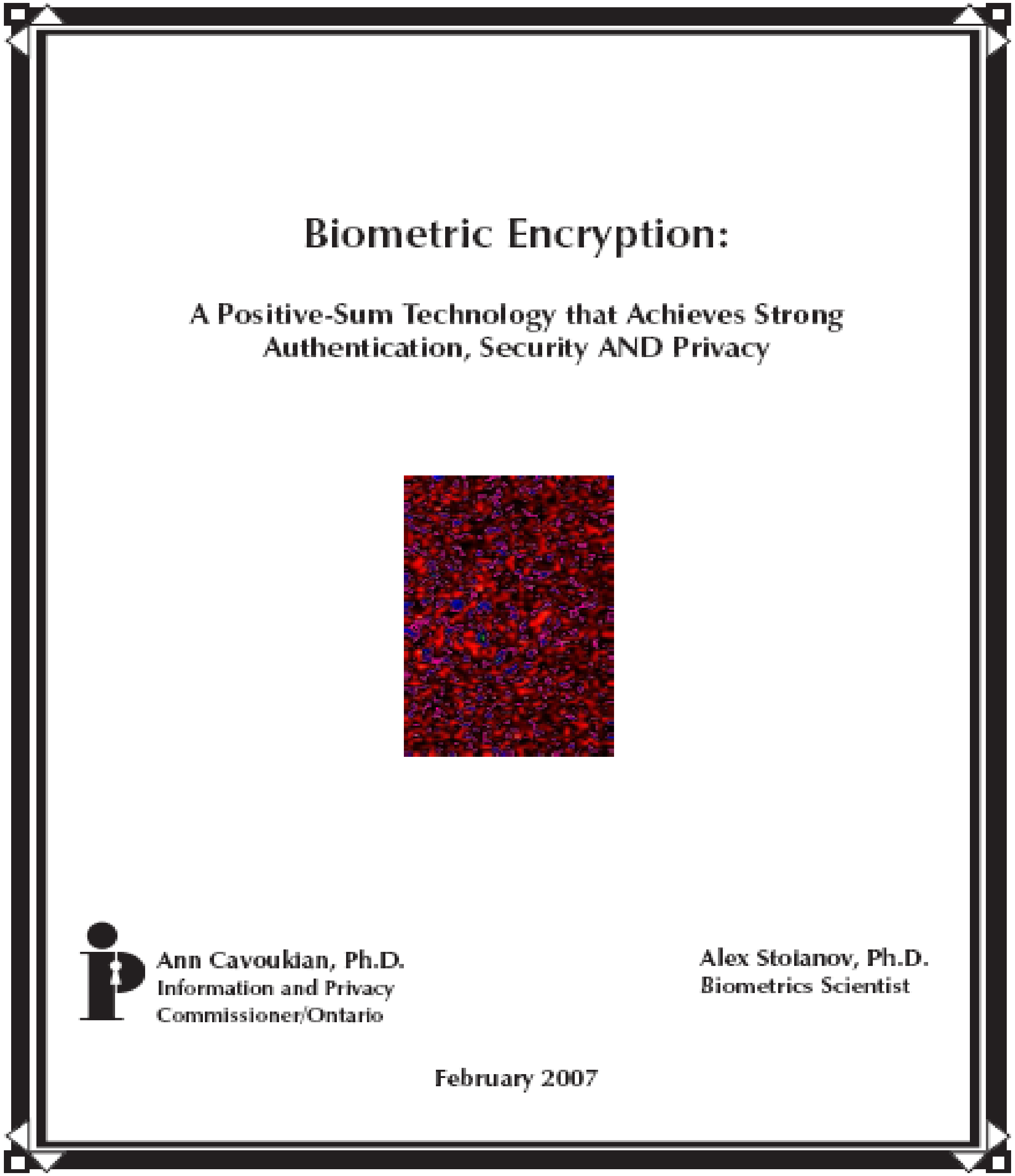
www.eubiometricforum.com

IPC

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 from the stored template. The key is recreated only if a correct 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 PINs can be 100s of digits in length because 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.

IPC Biometrics White Paper



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

IPC

IPC Biometrics White Paper (Cont'd)

- The IPC is developing a paper with chief scientist, Alex Stoinov, on the privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of ***biometric encryption technology***;
- The paper is intended to engage a broader, non-technical audience in considering the merits of the biometric encryption approach to verifying identity, ensuring strong security, and protecting privacy;
- I introduced the outline of our paper to IBAC at a meeting on December 12, 2006, and received widespread support from the technology companies in attendance;
- This paper was pre-released to IBAC on February 14, 2007, and will be released widely in March.

Conclusion

- Wherever possible, embed privacy into the design of the technology used: ***“Privacy by Design;”***

- “Privacy by Design” enhances and enables security. Do not get caught in the privacy vs. security mind set – ***you need both;***

- Encryption should be the default state for personal information at rest;

- An entirely new identity metasystem may be needed to deal with an expanded online population where fraud is proliferating;

- Consider the ***“Privacy-Embedded” 7 Laws of Identity*** as fundamental design principles;

- The most privacy-protective use of a biometric is one that does not have a template retained in a central database – ***consider biometric encryption.***

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) 326-3333 / 1-800-387-0073**
Web:	**www.ipc.on.ca**
E-mail:	**info@ipc.on.ca**