## Privacy by Design: The Gold Standard

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

Standing Committee on Access to Information, Privacy and Ethics

June 7, 2012



www.privacybydesign.ca

## Adoption of "Privacy by Design" as an International Standard

## Landmark Resolution Passed to Preserve the Future of Privacy

By Anna Ohlden - October 29th 2010 - http://www.science20.com/newswire/landmark\_resolution\_passed\_preserve\_future\_privacy

JERUSALEM, October 29, 2010 – A landmark Resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was unanimously passed by International Data Protection and Privacy Commissioners in Jerusalem today at their annual conference. The resolution ensures that privacy is embedded into new technologies and business practices, right from the outset – as an essential component of fundamental privacy protection.

### **Full Article:**

http://www.science20.com/newswire/landmark\_resolution\_passed\_preserve\_future\_privacy

# Privacy by Design: Proactive in 25 Languages!

1.English	9.Hebrew	17.Russian
2.French	10.Hindi	18.Romanian
3.German	11.Chinese	19.Portuguese
4. Spanish	12.Japanese	20.Maltese
5.Italian	13.Arabic	21.Greek
6.Czech	14.Armenian	22.Macedonian
7.Dutch	15.Ukrainian	23.Bulgarian
8. Estonian	16.Korean	24.Croatian
		25.Polish

## Privacy by Design: The 7 Foundational Principles

- 1. Proactive not Reactive:Preventative, not Remedial;
- 2. Privacy as the *Default* setting;
- 3. Privacy *Embedded* into Design;
- 4. Full Functionality:
  Positive-Sum, not Zero-Sum;
- 5. End-to-End Security:

  Full Lifecycle Protection;
- 6. Visibility **and** Transparency: Keep it **Open**;
- 7. Respect for User Privacy: Keep it **User-Centric**.



### Privacy by Design

#### The 7 Foundational Principles

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

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS Plus — taking a positive-sum (full functionality) approach, not zero-sum. That's the "Plus" in PETS Plus: positive-sum, not the either/or of zero-sum (a fake dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of Privacy by Design — ensuring privacy and gaining personal control over one sinformation and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (see over page):

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

### Made-in-Ontario Privacy Solution

# Facial Recognition Technology using Biometric Encryption

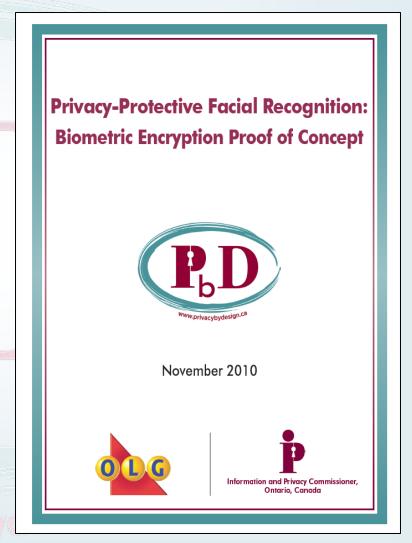
Www.privacybydesign.ca

### Social Media and Facial Recognition Technology

- Both Google and Facebook have added facial recognition technologies to their social media platforms in the U.S.;
- I have voiced my concerns to both about the collection of an individual's facial image which is a biometric identifier;
- I have also urged Google and Facebook to adopt a *Privacy by Design* solution that embeds privacy directly into their facial recognition technologies, resulting in privacy *and* functionality.

## Biometric Encryption: The Privacy by Design Approach

"The rapid, accurate identification and authentication of individuals has become a challenge across many sectors and jurisdictions ... Increasingly, biometric encryption is being viewed as the ultimate means of authentication or identification across a broad range of applications."



www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf

### **OLG Self-Exclusion program**

- Completely voluntary self-excluded gamblers program
   15,000 in Ontario and growing;
- **Great need** for reliable detection of those attempting to enter a gaming site against their wishes manual comparison alone in ineffective;
- Privacy of all casino patrons must be protected;
- Solution: Facial recognition in watch-list scenario through the use of *Biometric Encryption*;
- Novel "Made in Ontario" PbD application: through the collaboration of OLG, IPC, UofT, and iView Systems.

### **Biometric Encryption**

- Uses a biometric to uniquely encrypt a PIN or alphanumeric, and only store the encrypted PIN;
- Since the biometric is used to encrypt different PINs for each application, no single biometric template or digital representation of the biometric, is generated or retained in a database (there are *no* biometric templates in the system);
- Thus, one's biometric can never serve as a unique identifier that may be used by others for secondary purposes it stays on your face, where it belongs.

### Biometric Encryption (Cont'd)

• The privacy threat of using a biometric (face or finger) for tracking or profiling purposes is eliminated since no biometric or digital template is created, which may then be stored in a database and tracked – with BE, no tracking is possible.

Www.privacybydesign.Ca

# Social Media, Facial Recognition Technology and Biometric Encryption

- The potential of an individual's facial image, *i.e.*, a biometric identifier, being misused grows exponentially when its use is widespread, e.g., social media;
- Solution: Privacy by Design and Biometric Encryption
   (BE) embedding privacy directly into technologies,
   resulting in privacy and full functionality;
- A system using biometric encryption is highly privacy protective, yet accurate and secure, while leaving no digital trail of biometric templates behind.

### **Conclusions**

- For strong privacy, lead with Privacy by Design;
- Deliver *both* privacy *and* social media; or any other functionality, in an empowering "win-win" paradigm;
- Proactively embed privacy as a core functionality: the future of privacy may depend on it.