


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



PbD

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!

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

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.



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.”

Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept



November 2010



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 is 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.

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.