

***La protection intégrée de la vie privée :
Une règle d'or***

Ann Cavoukian, Ph.D.
**Commissaire à l'information et à la
protection de la vie privée**
Ontario, Canada

*Comité permanent de l'accès à l'information, de la protection des
renseignements personnels et de l'éthique – 7 juin 2012*



PbD

www.privacybydesign.ca
www.privacybydesign.ca

Adoption de la « protection intégrée de la vie privée » comme norme internationale

Adoption d'une résolution marquante pour protéger la vie privée dans l'avenir

Par Anna Ohlden – 29 octobre 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

JERUSALEM, 29 octobre 2010 – Les commissaires internationaux à la protection des données et de la vie privée, réunis à Jérusalem à l'occasion de leur conférence annuelle, ont adopté à l'unanimité une résolution marquante d'Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario. Cette résolution appelle l'intégration de fonctions de protection de la vie privée dans les nouvelles technologies et pratiques internes dès leur conception comme élément fondamental de la protection de la vie privée.

Article intégral (en anglais) :

http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

La protection intégrée de la vie privée : **proactive dans 25 langues!**

- | | | |
|-----------------------|----------------------|-----------------------|
| <i>1. Anglais</i> | <i>9. Hébreu</i> | <i>17. Russe</i> |
| <i>2. Français</i> | <i>10. Hindi</i> | <i>18. Roumain</i> |
| <i>3. Allemand</i> | <i>11. Chinois</i> | <i>19. Portugais</i> |
| <i>4. Espagnol</i> | <i>12. Japonais</i> | <i>20. Maltais</i> |
| <i>5. Italien</i> | <i>13. Arabe</i> | <i>21. Grec</i> |
| <i>6. Tchèque</i> | <i>14. Arménien</i> | <i>22. Macédonien</i> |
| <i>7. Néerlandais</i> | <i>15. Ukrainien</i> | <i>23. Bulgare</i> |
| <i>8. Estonien</i> | <i>16. Coréen</i> | <i>24. Croate</i> |
| | | <i>25. Polonais</i> |

Protection intégrée de la vie privée :

Les 7 principes fondamentaux

1. Prendre des mesures *proactives* et non *réactives*;
des mesures préventives et non correctives;
2. Assurer la protection *implicite* de la vie privée;
3. *Enchâsser* la protection de la vie privée dans la conception des systèmes et des pratiques;
4. Assurer une fonctionnalité *intégrale* selon un paradigme à somme positive et non à somme nulle;
5. Assurer la *sécurité* de bout en bout pendant *toute* la période de conservation des renseignements;
6. Assurer la visibilité et la transparence;
ouverture;
7. Respect de la vie privée des utilisateurs;
axée sur les utilisateurs.



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 false 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's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (*see over page*):

*Une solution de protection intégrée de la
vie privée adaptée aux besoins de
l'Ontario*

*Reconnaissance des visages au
moyen du chiffrement biométrique
que permet la protection intégrée
de la vie privée*

Médias sociaux et technologie de reconnaissance des visages

- Google et Facebook ont tous deux ajouté les technologies de reconnaissance des visages dans leurs plateformes de médias sociaux aux États-Unis.
- J'ai fait part de mes préoccupations aux deux concernant la collecte de l'image faciale de particuliers – un identificateur biométrique.
- J'ai aussi pressé Google et Facebook d'adopter une fonction de *protection intégrée de la vie privée* qui enchâsse la protection de la vie privée directement dans leurs technologies de reconnaissance des visages, assurant protection de la vie privée *et* fonctionnalité.

Chiffrement biométrique :

L'approche de la protection intégrée de la vie privée

« L'identification et l'authentification rapides et précises des particuliers sont devenues un véritable défi dans de nombreux secteurs et territoires. De plus en plus, le chiffrement biométrique est considéré comme le moyen ultime d'authentification ou d'identification dans un large éventail d'applications. »

**Privacy-Protective Facial Recognition:
Biometric Encryption Proof of Concept**



November 2010



Programme d'auto-exclusion d'OLG

- Programme totalement volontaire – 15 000 personnes ayant des problèmes de jeu en Ontario, et ce nombre ne cesse d'augmenter;
- **Besoin pressant** d'un moyen fiable de détecter les joueurs qui tentent d'entrer dans un établissement de jeu contre leur propre volonté; la comparaison manuelle seule s'est révélée inefficace;
- La vie privée de tous les clients des casinos doit être protégée;
- **Solution** : Reconnaissance des visages dans un scénario supposant une liste de surveillance au moyen du *chiffrement biométrique*;
- Application innovante et *adaptée aux besoins de l'Ontario* de la *protection intégrée de la vie privée* avec la collaboration d'OLG, de l'Université de Toronto, du CIPVP et de iView Systems.

Chiffrement biométrique

- Utilisation de caractéristiques physiques uniques pour chiffrer un NIP ou un code alphanumérique et stocker uniquement le NIP chiffré;
- Comme les données biométriques sont utilisées pour chiffrer différents NIP pour chaque application, aucun gabarit ni aucune représentation numérique des données biométriques n'est généré ou conservé dans une base de données (il n'y a *pas* de gabarits biométriques dans le système);
- Donc, les données biométriques d'une personne ne peuvent jamais servir d'identificateur unique que d'autres peuvent utiliser à des fins secondaires; elles restent à leur place, soit sur votre visage ou vos doigts.

Chiffrement biométrique *(suite)*

- La menace à la protection de la vie privée que représente l'utilisation de données biométriques (faciales ou digitales) à des fins de suivi ou de comparaison est donc éliminée puisque absolument aucun gabarit biométrique ou numérique n'est créé (pour être ultérieurement stocké dans une base de données et retracé). Avec le chiffrement biométrique, aucun suivi n'est possible.

Médias sociaux, technologie de reconnaissance des visages et chiffrement biométrique

- La possibilité que l'image faciale d'une personne, *c.-à-d.* un identificateur biométrique, soit utilisée à mauvais escient augmente de façon exponentielle lorsque son utilisation est généralisée (p. ex., médias sociaux en ligne);
- Solution : *Protection intégrée de la vie privée* et chiffrement biométrique – enchâssement de la protection de la vie privée directement dans les technologies, assurant protection de la vie privée *et* fonctionnalité complète;
- Un système qui utilise le chiffrement biométrique protège très bien la vie privée tout en étant précis et sûr, sans laisser de traces numériques de gabarits biométriques.

Conclusions

- Pour une protection rigoureuse de la vie privée, utiliser la *protection intégrée de la vie privée*;
- Offrir protection de la vie privée *et* médias sociaux, ou toute autre fonctionnalité, dans un paradigme habilitant où tout le monde est doublement gagnant;
- Enchâsser la protection de la vie privée de manière proactive pour assurer une fonctionnalité intégrale; l'avenir de la protection de la vie privée pourrait en dépendre.