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

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!

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

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**.

PbD

www.privacybydesign.ca

La protection intégrée de la vie privée

Les sept principes fondamentaux

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

La *protection intégrée de la vie privée* est un concept que j'ai élaboré dans les années 1990 en réponse aux effets systémiques toujours croissants des technologies de l'information et des communications et de la mise en place de grands systèmes de données réseautés.

La *protection intégrée de la vie privée* est fondée sur le principe selon lequel la protection de la vie privée ne pourra être assurée par le simple respect des lois et règlements et doit, idéalement, être intégrée dans les activités de l'organisation.

On croyait au départ que l'implantation de technologies de protection de la vie privée (TPVP) serait une bonne solution. Aujourd'hui, on se rend compte qu'il y a lieu d'adopter une démarche plus rigoureuse en implantant des *technologies de protection de la vie privée rehaussées* (TPVPR) selon une approche à somme positive (axée sur l'ensemble des fonctionnalités) et non à somme nulle. D'où le qualificatif « rehaussées », qui reflète l'abandon de la fausse dichotomie du paradigme à somme nulle.

La *protection intégrée de la vie privée* s'applique à un trio d'applications globales : 1) les systèmes informatiques; 2) des pratiques responsables; 3) la conception des systèmes et l'infrastructure des réseaux.

Les principes de la *protection intégrée de la vie privée* peuvent s'appliquer à tous les types de renseignements personnels, mais ils devraient l'être avec une rigueur particulière aux données délicates telles que les renseignements médicaux et financiers. Plus les données sont délicates, plus les mesures de protection de la vie privée tendent à être strictes.

Les objectifs de la *protection intégrée de la vie privée*, c'est-à-dire assurer la protection de la vie privée, exercer un contrôle sur les renseignements qui nous concernent et permettre aux organisations de se donner un avantage concurrentiel appréciable, peuvent être réalisés en respectant les sept principes fondamentaux suivants *(voir la page suivante)* :

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

Une solution adaptée aux besoins de l'Ontario en matière de protection de la vie privée

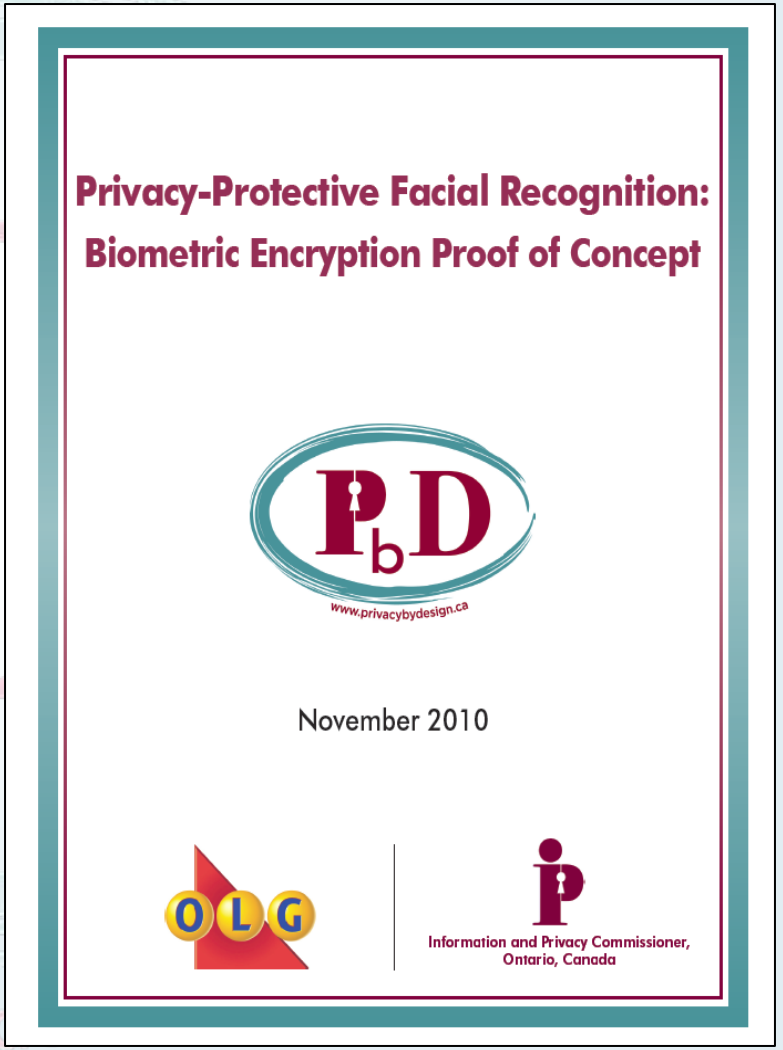
Reconnaissance biométrique des visages

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, qui constitue 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. »



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

Programme d'auto-exclusion d'OLG

- Programme totalement volontaire – 15 000 joueurs 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 n'est pas efficace;

- La vie privée de tous les clients des casinos doit être protégée;

- **Solution :** Reconnaisse 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, du CIPVP, de l'Université de Toronto 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.

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 profilage est donc éliminée puisqu'aucun gabarit biométrique ou numérique n'est créé pour être ensuite 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);
- 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 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.