

PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of
Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29^e Conférence internationale des commissaires
à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

Rendre la protection de la vie privée opérationnelle

Mettre à jour le Cadre de la protection de la vie privée de l'ISTPA

John T. Sabo

Président, International Security Trust and
Privacy Alliance (ISTPA)

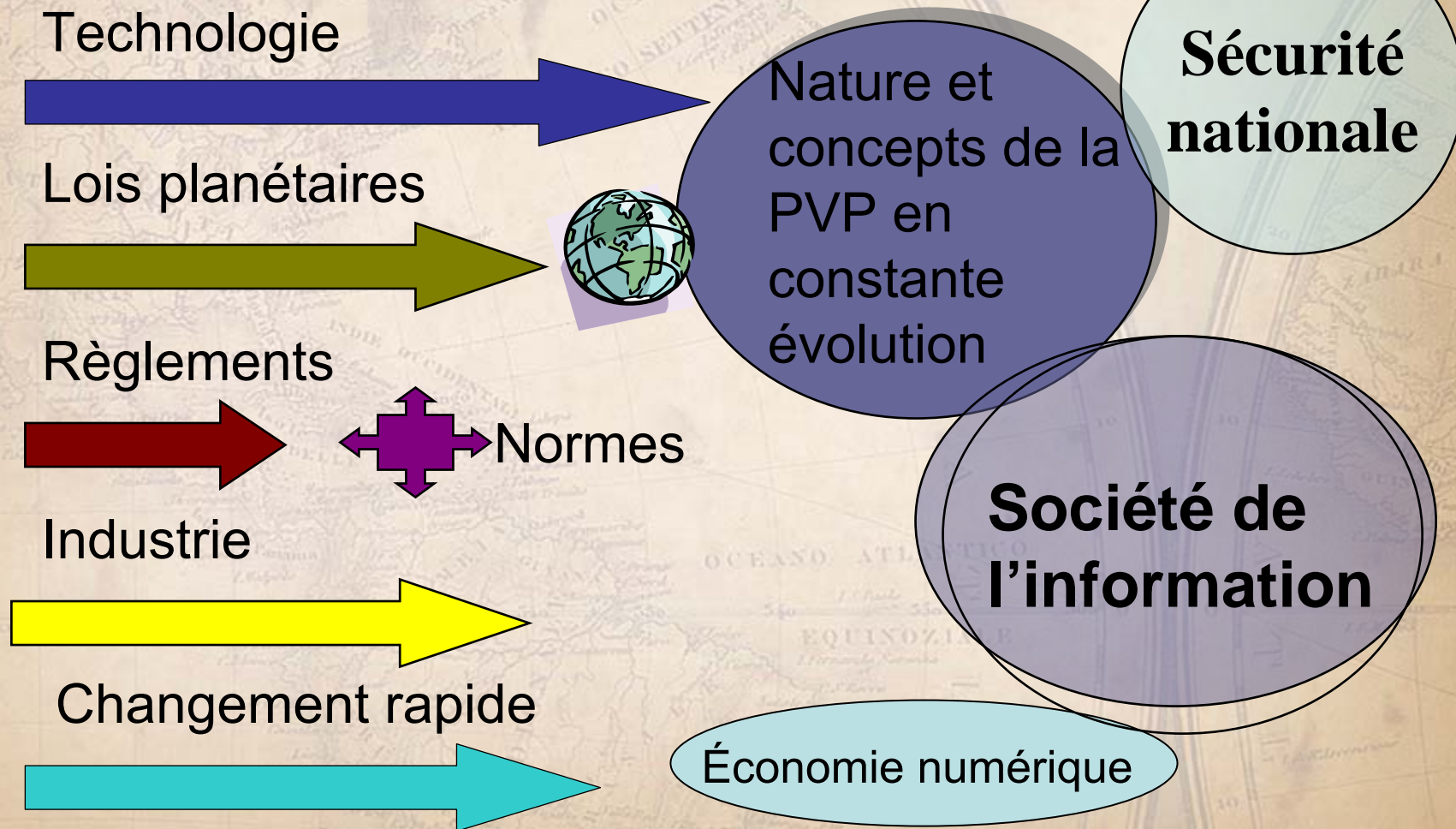
Directeur, Global Government Relations CA, Inc.



Qu'est-ce que l'ISTPA?

- La International Security, Trust, and Privacy Alliance, fondée en 1999, est un regroupement global de sociétés, institutions et fournisseurs de technologie qui travaillent en collaboration pour clarifier et résoudre des problèmes actuels et à venir liés à la sécurité, à la confiance et au respect de la vie privée.
- La priorité de l'ISTPA est la protection des renseignements personnels (RP)
- Voir le site à www.istpa.org

La protection de la vie privée (PVP) : Une réalité complexe et stimulante



Politiques et lois mondiales en matière de PVP – de vastes écarts

Principes de PVP de l'OCDE

Pratiques équitables de traitement de l'information

La HIPAA

Cadre de PVP de l'APEC

U.S. Privacy Act

Directive relative à la protection des données à caractère personnel de l'UE

Code type sur la protection des renseignements personnels de la CSA



Point de vue de l'ISTPA sur la PVP

- Aspect opérationnel – Priorité accordée aux solutions
 - Passer à la discipline de l'ingénierie de la PVP
 - Cadre de PVP à l'appui de tout le cycle de vie de la PVP
 - *N'est pas un cadre de politique* – c'est plutôt un cadre technique aux fins des processus administratifs et à l'appui des systèmes de TI
- Plateforme aux fins de la collaboration multidisciplinaire
- Doit tenir compte des variantes dans les lois et politiques
- Cas d'utilisation propres à l'industrie

Cadre de l'ISTPA – Concepts v 1.1

- Un ensemble ouvert de services et de possibilités de collaboration configurable selon les politiques utilisé pour éclairer l'analyse, la conception, la mise en application et l'évaluation de solutions et d'infrastructure relatives à la PVP
- Une approche architecturale qui fournit un modèle utilisable par les architectes de la TI et les gestionnaires de programme afin d'élaborer des applications interexploitables

PVP selon l'ISTPA – Cadre v 1.1

Services

- **Contrôle** – politique – gestion des données
- **Certification** – justificatif d'identité, processus sécurisés
- **Interaction** – gère les données/préférences/avis
- **Négociation** – des accords, règles, privilèges
- **Agent** – logiciel qui exécute les processus
- **Usage** – utilisation des données, agrégation, préservation de l'anonymat
- **Vérification** – indépendante, responsabilisation vérifiable
- **Validation** – vérification de l'exactitude des renseignements personnels
- **Application** – y compris les mesures de réparation dans les cas d'infraction
- **Accès** – sous toute réserve/mise à jour des renseignements personnels

Cadre de l'ISTPA remis en tant que spécification ISO publiquement disponible

- Soumis par l'ISSEA (International Systems Security Engineering Association) en octobre 2003-2004
- Le scrutin devait prendre fin le 11 décembre 2004
- A donné lieu à d'importantes discussions, notamment à la création du groupe d'études sur la technologie relative à la PVP dans le cadre de l'ISO JTC-1
- Retrait demandé le 22 novembre 2004 afin d'effectuer le travail additionnel

Travail récent : « Analyse des principes de la PVP : rendre la PVP opérationnelle »

- Choisir des directives et lois globales représentatives en matière de PVP
- Analyser les variations en matière de langues et de définitions et les besoins exprimés
- Faire l'analyse des besoins et les transformer en « principes » de PVP opérationnels
- Faire une liste de correspondances et déterminer les besoins communs et les cas particuliers.

Lois, directives et codes choisis

- La Privacy Act adoptée en 1974 (É.-U.)
- Lignes directrices sur la PVP de l'OCDE
- Lignes directrices de l'ONU
- Directive relative à la protection des données à caractère personnel de l'UE
- Code type de l'Association canadienne de normalisation
- Health Insurance Portability and Accountability Act (HIPAA)
- US FTC Fair Information Practice Principles
- Principes de la sphère de sécurité É.-U.-UE
- Australian Privacy Act
- Loi du Japon sur la protection des renseignements personnels
- Cadre de la PVP de l'APEC
- California Security Breach Bill

Principes de PVP de base

- **Responsabilisation**
 - **Avis**
 - **Consentement**
 - **Limite de la collecte**
 - **Limite d'utilisation**
 - **Communication**
 - **Accès et correction**
 - **Sécurité/mesures de protection**
 - **Qualité des données**
 - **Application**
 - **Ouverture**
- En plus :*

 - **Anonymat**
 - **Flux de données**
 - **Sensibilité**

Exemple : « Le principe relatif à l'avis » comprend :

- ◆ La définition des renseignements personnels recueillis
- ◆ Son utilisation (préciser le but)
- ◆ Sa communication à des personnes à l'intérieur ou à l'extérieur de l'entité
- ◆ Les pratiques associées à la conservation et à la protection de l'information
- ◆ Les possibilités qui s'offrent à la personne sur laquelle portent les données en ce qui concerne les pratiques de PVP de celui ou celle qui recueille les données
- ◆ Les changements apportés aux pratiques ou aux politiques
- ◆ Les informations fournies à la personne sur laquelle portent les données dans des situations et à des moments précis

Prochaines étapes : Démarche à suivre en matière de PVP selon l'ISTPA Cadre v 2.0

- Utiliser l'étude sur l'*analyse* afin d'évaluer le cadre existant – tout le document est accessible en ligne
- *L'analyse* est employée par les organismes externes
- Terminer l'élargissement des fonctions du cadre, y compris la fonction étiquetage
- Poursuivre la collaboration avec l'ISSEA en ce qui concerne la cartographie de la sécurité
- Continuer l'élaboration du projet de Boîte à outils prototypes pour rendre le cadre plus accessible et utilisable
- Ébauche prévue de la version 2.0 : 2008

Des questions?

john.t.sabo@ca.com



www.istpa.org