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

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

du 25 au 28 septembre 2007
Montréal, Canada

« Dire ce que l'on fait et faire ce que l'on dit » : Arguments et observations en faveur d'une norme internationale de protection des renseignements personnels

Colin J. Bennett
Département de science politique
Université de Victoria (C.-B.)
cjb@uvic.ca
Robin Bayley
Linden Consulting Inc., Victoria (C.-B.)
rmbayley@shaw.ca

Pourquoi les organisations certifiées ISO 9001 devraient avoir de meilleures pratiques de gestion des renseignements personnels

- Les organisations ont une meilleure compréhension de leurs systèmes d'exploitation et de leurs fonds de données personnelles.
- Leur personnel est formé.
- Les organisations doivent réfléchir et répondre aux exigences réglementaires.
- Les organisations peuvent tirer parti d'une expertise extérieure grâce au processus d'évaluation de la conformité.

Exigences liées à une norme de gestion de la protection des renseignements personnels

- Traduction des principes relatifs à l'équité dans le traitement des renseignements dans une langue et une forme propres aux normes
- Prestation de conseils pour la mise en œuvre des principes dans les organisations
- Outils d'évaluation de la conformité adaptés à la taille de l'entreprise et à la sensibilité des données
- Guide de vérification
- Système d'accréditation pour les vérificateurs spécialisés dans la protection des renseignements personnels

Chevauchement entre la gestion de la qualité et la protection des données

- Transparence de la politique et de l'objectif
- Procédures liées à l'interaction avec les sujets des données
  - Règlement des plaintes
  - Demandes d'accès et de correction
  - Disposition concernant le consentement et le retrait
- Procédures de gestion des données personnelles
  - Sécurité des données
  - Qualité des données
  - Conservation des données

Motivations pour l'adoption de normes de protection de la vie privée

- Pouvoirs d'éducation et de réglementation des autorités de protection des données
- Désir de bénéficier d'un avantage concurrentiel
- Capacité de mentionner la norme dans les contrats

Initiatives visant la normalisation de la gestion de la protection des renseignements personnels

- Organismes de normalisation nationaux
  - Association canadienne de normalisation (CSA)
  - American National Standards Institute (ANSI)
- Organisation internationale de normalisation (ISO)
  - Travail du groupe JTC-1 de l'ISO et de la Commission électrotechnique internationale (CEI)
- Comité européen de normalisation/Système de normalisation de la société de l'information
- International Security, Trust and Privacy Alliance (ISTPA)

Séance d'information sur les normes

John Hopkinson, ISSPCS-spécialiste CISSP, ISP, CDRP

Stratège en sécurité, EWA /IIT

Président de l'ISSEA

Président du CCC-JTC1/CTTI

JTC 1/ISO/CEI

- JTC 1 est unique
  - C'est une norme hybride de l'ISO et de la CEI
  - 30 % des clients sont d'autres concepteurs de normes
  - Il produit des « normes de base »
  - Il doit toujours prendre en considération la « pire éventualité »
- A élaboré des normes liées à la protection de la vie privée (PVP) au cours des 7 à 10 dernières années

JTC 1/SC 17/ISO/CEI

- Se préoccupe de la PVP concernant les applications utilisant la technologie des cartes
- Comprend des données sur la carte à puce et la carte optique
- N'examine pas actuellement les normes relatives à la PVP
- Le président est l'auteur de deux évaluations des facteurs relatifs à la vie privée concernant la technologie des cartes évoluées

JTC 1/SC 27/ISO/CEI

- A créé un nouveau groupe de travail pour la PVP dont les projets portent sur :
  - Le cadre de la PVP
  - L'architecture de référence de la PVP
  - Des infrastructures de la PVP
  - L'anonymat et les justificatifs d'identité
  - Les technologies permettant d'accroître la protection de la vie privée
  - L'ingénierie de la PVP

JTC 1/SC 31/ISO/CEI

- Élabore des normes pour les dispositifs d'IRF
- Commence à prendre en considération la PVP
- A ajouté la fonction « bit d'arrêt » à la norme ISO/CEI 18000-6
- Les blocs mémoire comprennent la protection par mot de passe

JTC 1/SC 32/ISO/CEI

- Des normes pour la gestion et l'échange des données, y compris le cybercommerce
- Porte sur les affaires électroniques, les métadonnées, les langages de base de données et les progiciels d'application et multimédia SQL
- Reconnaît « l'individu » comme un sous-type de personne, qui a des droits que les normes des cybercommerces doivent respecter

JTC 1/SC 36/ISO/CEI

- Normes d'apprentissage, d'éducation et de formation
- Appuient les exigences juridiques
- Faire enquête auprès des membres pour connaître les exigences particulières à leur pays
- Norme la plus importante
  - ISO/CEI 24751 – Adaptabilité personnalisée et accessibilité en matière d'apprentissage, d'éducation et de formation électroniques

JTC 1/SC 37/ISO/CEI

- Élabore des normes pour la biométrie
- A commencé à se pencher sur la PVP
- Travaille sur
  - les aspects interorganisationnels et sociétaux de la mise en application des technologies biométriques
  - un guide sur l'accessibilité, la PVP et les questions de santé et de sécurité dans la mise en place de systèmes biométriques pour application commerciale

Autres élaborations de normes

- Plusieurs consortiums sont actifs :
  - ISSEA
  - ISTPA
  - SSSIB
  - OMG
  - W3C
- Il y en a probablement plusieurs autres

Stratégie canadienne de normalisation de la PVP

- 21 et 22 février 2007 : CPVP, CSA, CCN, ONGC
- Feuille de route de la normalisation de la PVP
  - Ce qui est disponible et ce dont on a besoin
- Rapport sur l'atelier
  - +, besoins particuliers, conformité, partager les pratiques exemplaires, important de choisir le bon moment, participation

PROBLÈMES

- **JTC 1/ISO/CEI et autres**
- Manque de coordination des activités liées à la PVP
- Aucun véritable point de convergence pour le travail sur la PVP
- Manque de principes de PVP harmonisés
- Besoin d'une communauté de la PVP et de coopération en matière de normes techniques

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

Technologie

Lois planétaires

Règlements

Normes

Industrie

Changement rapide

Nature et concepts de la PVP en constante évolution

Sécurité nationale

Société de l'information

Économie numérique

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