

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

La circulation et le miroitage de données

Martin Abrams
Septembre 2007

mabrams@huron.com

972.781.6667

Nous sommes à l'aube d'une révolution de l'information

- Le volume d'information augmente de façon géométrique.
 - Aujourd'hui, nous parlons d'exaoctets de données, alors qu'hier, nous parlions de téraoctets et avant hier, de gigaoctets.
 - Les processus de traitement des données contribuent à accroître le nombre de données que nous pouvons comprendre à l'aide des ordinateurs.
 - Donc, les données utilisables augmentent également de façon géométrique.

Nous sommes à l'aube d'une révolution de l'information (suite)

- Les rapports analytiques s'améliorent également à un taux géométrique.
 - L'information a davantage de valeur.
- Les nouvelles économies stimulent la croissance en créant des emplois axés sur le savoir.
- L'amélioration des communications signifie que l'on peut concentrer les efforts là où ils sont le plus efficaces.

La circulation des données sur une période de dix ans

1997

- Les données sont transférées au moyen de cassettes ou de disques.
- Les données sont conservées et traitées au même endroit.
- L'accès aux données se fait à l'endroit où les données sont conservées.
- Il y a un petit réseau de préposés au contrôle et au traitement.
- La réglementation ne pose pas un trop gros défi.

La circulation des données sur une période de dix ans

2007

- Les données circulent par voie électronique.
- Les données sont traitées à distance et à plusieurs endroits en même temps.
- L'accès aux données peut se faire n'importe où.
- Il y a une longue chaîne de contrôleurs et de sous-traitants, qui ajoutent tous de la valeur.
- Les défis sont complexes.

En quoi consiste un transfert aujourd'hui?

- Un service à la clientèle offert 24 heures par jour, 7 jours par semaine.
- Le traitement d'un paiement pour un achat fait en Chine au moyen d'une carte émise en Allemagne et à partir d'un téléphone dans une chambre d'hôtel au Canada.
- Restructuration des processus commerciaux en Inde.
- Établissement d'équipes de projet en Espagne, en Russie, en Chine, en Australie, aux États-Unis et au Canada.
- Établissement de réseaux sociaux dans une collectivité mondiale.

Exemple d'établissement d'équipes composées de membres de la collectivité mondiale

- Une équipe est créée pour résoudre un problème médical.
 - Des docteurs et des scientifiques de dix pays, spécialisés dans divers domaines, travaillent au sein d'une équipe virtuelle.
 - De nouveaux membres peuvent s'ajouter.
- Tous doivent examiner les mêmes ensembles de données.

Exemple d'établissement d'équipes composées de membres de la collectivité mondiale (suite)

- Les ensembles de données comprennent :
 - des données cliniques;
 - des données épidémiologiques;
 - des données sur des composés et des matériaux.
- Les données sont stockées dans les serveurs des dix pays mais elles sont réfléchies sur chaque écran.
- À quel système de réglementation cette équipe est-elle assujettie?

La nature même de la protection de la vie privée complexifie notre problème

- La protection de la vie privée est d'ordre local.
 - Protection des renseignements personnels
 - Domaine de l'autonomie
 - Sécurité
- La circulation des données est du domaine mondial.
- Pourtant, les personnes exigent que l'on satisfasse à leurs attentes d'ordre local dans un monde de plus en plus réseauté.

Nouveau modèle de gouvernance

- La protection de la vie privée est une préoccupation locale.
- Les données circulent dans le monde entier.
- Les obligations sont universelles.
 - Systèmes de gouvernance axés sur la responsabilisation
 - Règles professionnelles contraignantes
 - Règles transfrontalières en matière de vie privée
 - Augmentation des agents et des méthodes de responsabilisation
 - Liens fondés sur des principes communs

Conclusion

- Le transfert et le miroitage de données sont une simple conséquence de la révolution de l'information et des communications.
- L'information sera un moteur de croissance et de changement.
- Les attentes des personnes doivent être satisfaites peu importe où les données sont consultées.
- Cela suppose des structures de gouvernance compatibles avec le fait que la vie privée est une préoccupation locale, que les données circulent dans le monde entier et que les obligations sont universelles.

La circulation et le miroitage de données

Benjamin S. Hayes

Chargé de la conformité aux mesures de protection des renseignements personnels des Amériques
Accenture, s.r.l.

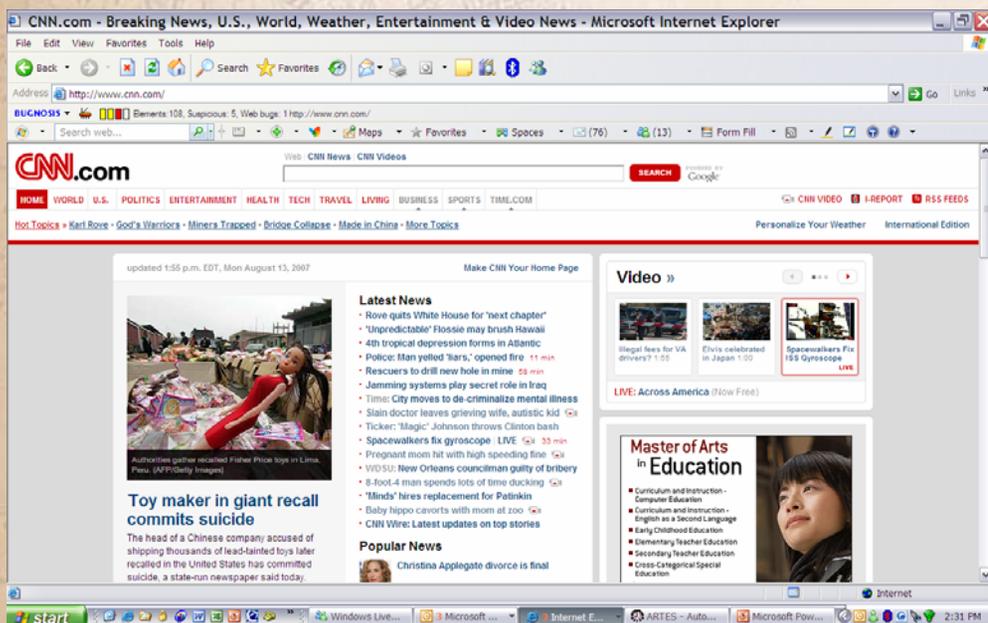
La circulation et le miroitage de données

- Quelles données franchissent les frontières, et où se rendent-elles?
- Pour quelles raisons les données circulent-elles?
Quelles sont les tendances?
- Prévisions pour l'avenir
- Impartition – mythes et réalités



Premier exemple : site Web commercial

Le contenu et les modules de fonctionnalité (à l'exception de la publicité sur le Web) fournis par diverses tierces parties :



- Dell
- Careerbuilder.com
- Google
- People magazine
- Yahoo
- Accuweather.com
- Time.com
- AOL
- Fortune
- Etc., etc., etc.

Site Web commercial (suite)

- À son tour, le fonctionnement de chaque module est probablement assuré par un fournisseur de services de Google, Time, AOL, etc.
- Ces fournisseurs de services peuvent impartir une partie ou l'ensemble de la fonctionnalité à un sous-traitant.
- Les données saisies par le biais d'un module peuvent être accessibles à de multiples parties dans de multiples régions.
- Pratiquement toutes les mesures de contrôle servant à protéger les données seront contractuelles (par opposition à la conformité aux lois).

Deuxième exemple – impartition en RH

- Les services offerts proposent normalement la majorité des fonctions de gestion du personnel :
 - la paie
 - l’inscription aux avantages
 - le changement de statut
 - la communication aux employés
 - la ligne secours pour les demandes d’employés

Façon dont un poste hypothétique d'officier des ressources humaines est doté

- Supposons que le client se trouve aux États-Unis, au R.-U., aux Pays-Bas et en Belgique.
 - L'entente peut être signée à Londres entre Client R.-U. et Accenture R.-U.
- Les conseillers d'Accenture se trouvent aux États-Unis, au R.-U., en Argentine et à Manille.
- Les centres d'appel sont situés à Buenos Aires, à Varsovie et à Kuala Lumpur, pour assurer un service continu.
- Le traitement des données se fait à Bangalore.
- L'impression et l'envoi se font par une tierce partie aux États-Unis.

Pourquoi les services sont-ils offerts ainsi?

- Raison principale – le coût
 - le souci d'efficacité et d'économies est un élément catalyseur de l'impartition
 - les entreprises publiques font l'objet de grandes pressions pour générer des profits pour les actionnaires
- Raisons secondaires –
 - la capacité de distribuer le travail à des équipes d'experts dans diverses régions
 - la capacité d'offrir un service 24 heures sur 24
 - les diverses langues parlées

Complexité accrue – l'infrastructure de communications

- Les serveurs sont situés dans des lieux de service, mais leur contenu est sauvegardé sur différents continents pour les besoins de reprise des activités après un sinistre.
- Les serveurs secondaires de réserve (capacité de reprise) peuvent se trouver dans un tout autre pays.
- L'équipe de prestation des services aux clients, dont les membres sont largement répartis, peut utiliser un site Web d'un groupe privé (hébergé à Chicago, entretenu à partir de l'Inde) pour collaborer à des projets, se communiquer des versions provisoires, etc.
- L'avènement de voix par IP pourrait obliger un réexamen des hypothèses concernant la protection et la sécurité des communications vocales – mise en cache, acheminement, paquets de texte en clair, etc.
- **Il serait donc nécessaire de mettre en vigueur un ensemble complexe de clauses types et d'autres ententes sur le transfert de données pour suivre les données, ce qui est très difficile à gérer.**

Prévisions pour l'avenir

- La diffusion de données et la segmentation des procédés opérationnels se font sous l'impulsion de l'économie et des améliorations dans les technologies de l'information. L'augmentation de la disponibilité de la bande passante va se poursuivre, ce qui aura comme effet d'accroître la diffusion de données et la segmentation des procédés opérationnels.
- Un nombre croissant d'entreprises auront recours au traitement non local des données au lieu de la fonction de contrôleur moderne.
- La réalité des affaires exige une gestion constante de données en provenance d'un grand nombre de sources – il y a donc un besoin économique de règles harmonisées à l'échelle internationale en ce qui concerne l'échange de données.
- Une réglementation accrue ou non harmonisée qui nuit à la circulation transfrontalière de données aura comme effet d'empêcher de bons rendements économiques.
- L'imposition de limites territoriales sur la circulation transfrontalière de données ne permettra pas vraiment de réduire les risques actuels – un régime de réglementation axé sur le risque (plutôt que territorial) protégerait mieux les intérêts des consommateurs.

Mythes de l'impartition



—Report, N. Y. Bureau of Statistics of Labor, 1885
Cloak shop on the top floor of 12 Hester St.

- Le travail s'effectue dans des conditions insalubres, par des personnes non scolarisées et indignes de confiance.
- Les normes de sécurité de l'information sont laxistes.
- Les données sont forcément moins protégées qu'elles ne le seraient dans leur pays d'origine.

Réalités de l'impartition



- Le travail s'effectue dans des conditions commerciales modernes par des personnes scolarisées, formées et présélectionnées.
- Les normes de sécurité de l'information sont extrêmement strictes.
- Les données sont plus protégées qu'elles pourraient l'être dans bien d'autres endroits.

Les centres d'exécution d'Accenture mettent l'accent sur les attentes en matière de sécurité et font l'objet d'une vérification

- Bangalore a reçu la certification de niveau 3 selon le eSourcing Capability Model for Service Providers (modèle de capacité en sourcing électronique pour les fournisseurs de services) par l'Université Carnegie Mellon – il s'agit du premier impartiteur au monde à recevoir cette désignation.
- Plus de 17 centres d'exécution d'Accenture feront l'objet de vérifications SAS 70 de niveau II en 2007.
- Huit centres sont actuellement conformes à la norme ISO 27001; trois autres le seront dès octobre 2007 (la plupart des centres d'exécution de services impartis d'Accenture); diverses autres certifications de normes en vigueur.
- Formation obligatoire sur la protection des renseignements pour le personnel à l'échelle mondiale.

CIRCULATION ET MIROITAGE DE DONNÉES

David Loukidelis

Commissaire à l'information et à la protection
de la vie privée

de la Colombie-Britannique

oipc.bc.ca

Nature évolutive de la circulation transfrontalière des données (CTD)

- Comme les autres membres du groupe d'experts l'ont observé, la nature, la complexité, l'ampleur et la portée de la circulation mondiale des données ont énormément changé en seulement 10 ans.
- L'économie actuelle garantit l'élargissement de la bande passante, la diminution des coûts de stockage et l'évolution continue des TIC.
- À mesure que nous avançons sur la nouvelle « route des épices » (Alhadeff), les modèles conventionnels de protection des données (PD) rencontrent des défis de plus en plus grands.

Défis posés aux mécanismes

conventionnels de responsabilisation

- Les gouvernements et les autorités de protection des données (APD) doivent depuis longtemps tenir compte des juridictions territoriales en ce qui concerne l'application de la loi en matière de PD.
- Au Canada, les limites constitutionnelles à l'autorité du gouvernement donne lieu à une mosaïque de lois similaires mais différentes sur la protection des renseignements personnels.
- En matière de CTD, les APD canadiennes font donc face à des défis nationaux semblables aux défis internationaux.
- L'harmonisation des lois canadiennes est souhaitable (à comparer avec l'approche de la Conférence des États-Unis pour l'harmonisation des lois).

Défis en matière de responsabilisation (suite)

- La collaboration entre les APD canadiennes est souhaitable, et de plus en plus une réalité dans les secteurs public et privé.
- Les gouvernements et les APD font face à des défis encore plus grands en matière de CTD à l'échelle internationale.
- Mis à part les limites des juridictions territoriales, la nature même des appareils judiciaires et des cadres réglementaires diffère, et des mésententes sont possibles.
- Tel a été le cas depuis le jour où nous avons effectué de simples transferts de lots de données.

Faire face aux défis

- Les lois de l'Union européenne rendent compte d'un cadre de contrôle d'exportation qui peut être perçu comme une façon de répondre aux défis de la CTD.
- Le Safe Harbor des États-Unis est un bon exemple des défis posés par des interventions différentes pour protéger la vie privée, dont l'une est le recours au cadre de contrôle d'exportation
- Une autre intervention possible est le recours aux clauses de contrat types (Union européenne et ICC)

Faire face aux nouveaux défis

- L'évolution constante et l'étendue de la CTD exigent de nouvelles solutions, car le cadre de contrôle d'exportation et les contrats types sont de moins en moins adaptés aux défis que posent la CTD.
- Que pouvons-nous faire?
- La question se pose déjà depuis un bon moment, et il n'y a pas qu'une seule réponse possible.

Collaboration en matière de réglementation

- La collaboration bilatérale des APD peut s'avérer utile dans des cas spécifiques (permet d'assouplir mais non d'éliminer les questions de juridictions). Prenons par exemple la collaboration Canada/États-Unis dans l'affaire Abika)
- L'échange de renseignements entre APD peut permettre une meilleure affectation des ressources d'application de la loi

Collaboration en matière de réglementation (suite)

- La collaboration multilatérale, c'est cela et bien plus, comme la création des ressources harmonisées pour aplanir les différences entre les divers cadres de protection de la vie privée.
- L'organisation des APD de l'Asie-Pacifique est un exemple de collaboration multilatérale dans un contexte international régional.

La collaboration, et quoi d'autre?

- Il y a évidemment des limites aux avantages de la collaboration : celle-ci ne peut pas éliminer les obstacles mentionnés plus tôt, dont le plus important reste les différences entre les cadres judiciaires et réglementaires.
- Ces obstacles motivent la recherche de nouvelles approches pour compléter ou remplacer les approches actuelles comme les contrats types et les contrôles d'exportation.

Systemes de protection transfrontalière des renseignements personnels (SPTRP)

- Mettons de côté les normes internationales (qui sont très bonnes en principe) : les SPTRP consistent en l'adoption de règles en matière de protection de la vie privée régissant la conduite internationale des entreprises.
- Une «norme internationale» comme le Cadre de protection de la vie privée de l'APEC pourrait soutenir les SPTRP.
- La prochaine étape pour l'APEC et d'autres organismes consiste à établir des systèmes de responsabilisation.

SPTRP (suite)

- Le défi consiste à trouver des approches différentes et complémentaires pour garantir la responsabilisation en matière de pratiques de protection de la vie privée dans le monde complexe de la CTD.
- Des agents de responsabilisation apposant des « marques de confiance » semblent prometteurs en ce qui a trait à l'élimination des obstacles territoriaux pour offrir un règlement alternatif des différends, des vérifications et des mécanismes de recours et pour compléter les mesures prises par les gouvernements et les APD.

Conclusion

- Les SPTRP sont prometteurs.
- Il faut poursuivre les travaux sur les normes internationales (l'OCDE, l'APEC et l'ISO se rencontrent?)
- Les APD peuvent et doivent accroître le niveau de collaboration à divers plans.
- Il n'y a pas de solution miracle, mais une gamme d'approches peut aider les intervenants à naviguer dans le nouveau monde de la CTD.