

TERRA INCOGNITA

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

Confronter les dragons internes et externes : Est-ce la frontière ultime de la protection de la vie privée?

Rapport sur Terra Incognita :
29^e Conférence internationale des commissaires à la protection
des données et de la vie privée

Montréal, Canada
25-28 septembre 2007

Par : Jane Bailey*, Ottawa

Le Commissariat à la protection de la vie privée du Canada a commandé le présent document. Les opinions qui y sont exprimées n'engagent que leur auteur sans nécessairement refléter le point de vue du Commissariat, ni celui du gouvernement du Canada.

* Jane Bailey est professeure adjointe à la Faculté de droit de l'Université d'Ottawa : jbailey@uottawa.ca. L'auteure remercie Ian Kerr, Khâled El Emam, Tim Caulfield et le personnel du CPVP pour leurs commentaires sur les versions précédentes du rapport, ainsi que Bridget McIlveen, Katie Black, Jena McGill et Julie Shugarman pour l'excellente documentation sur la conférence. L'auteure remercie également le Commissariat à la protection de la vie privée du Canada de lui avoir donné l'occasion de présenter un rapport sur cette conférence sans précédent ainsi que Michael Geist et tous les autres conférenciers pour leurs exposés informatifs et inspirants.

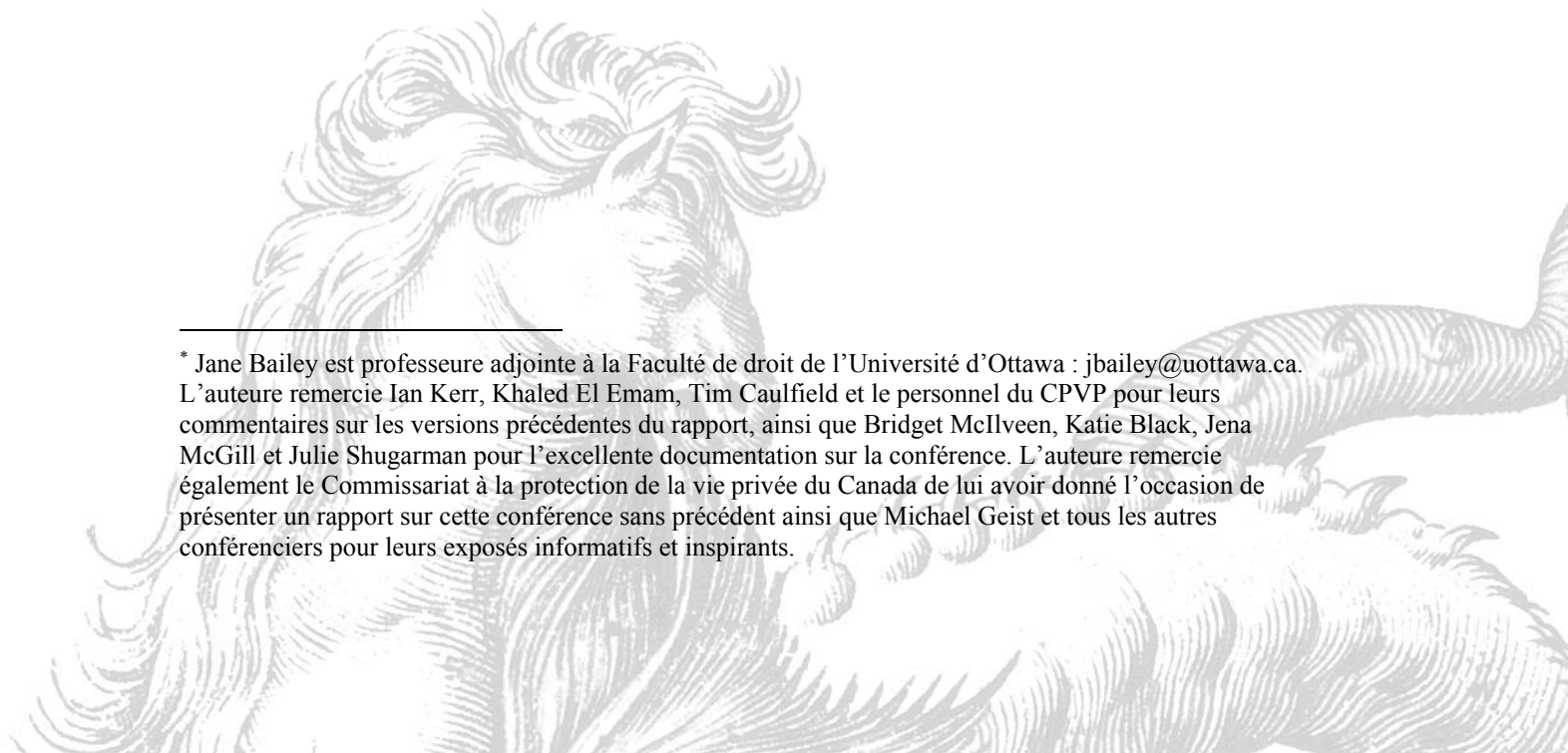


TABLE DES MATIÈRES

INTRODUCTION	4
I. LES DRAGONS	5
A. Mondialisation	5
(i) Sécurité publique	5
(ii) Circulation et miroitage de données d'une frontière à l'autre	6
(iii) Difficultés intergouvernementales	7
B. Technologie	8
(i) Forage de données	8
(ii) Identification par radiofréquence (IRF)	9
(iii) Repérage géodépendant	10
(iv) Génétique et mise en banque de substances biologiques	11
(v) Informatique ubiquiste	12
(vi) Nanotechnologie	13
(vii) Établissement de normes	14
C. Prochaine génération	15
D. Crimes sur Internet	16
II. TUEURS DE DRAGONS/DOMPTEURS DE DRAGONS/COALITION CONTRE LES DRAGONS	17
A. Collaboration multisectorielle et intergouvernementale	18
(i) Initiatives de Londres en 2006, de l'APEC et de l'OCDE	18
(ii) Planification de la protection des renseignements personnels dans le travail de conception	19
(iii) Initiatives de la société civile	20
B. Sceaux de confidentialité	21
C. Dépersonnalisation	22
D. Vérifications	23
E. Évaluations des facteurs relatifs à la vie privée (ÉFVP)	25
III. THÈMES RÉCURRENTS	26
A. Le sens de la protection de la vie privée	26
B. Protection de la vie privée et sécurité	28
C. Incohérences dans les approches juridiques existantes	29
(i) Modèles fondés sur le consentement, le contrôle et la propriété	30
(ii) Règle juridique fondée sur les territoires physiques	31

(iii) Efforts axés sur la conservation et l'utilisation plutôt que sur la réduction	31
(iv) Caractère inadéquat du modèle hiérarchique canadien	32
CONCLUSION	33
ANNEXE A – Résolution sur l'urgence d'établir des normes mondiales concernant la protection des données des passagers dont se serviront les gouvernements à des fins d'application de la loi et de sécurité frontalière, 29 ^e Conférence internationale des commissaires à la protection des données et de la vie privée, Montréal, Canada (25-28 septembre 2007)	34
ANNEXE B – Déclaration des organisations de la société civile sur le rôle des commissaires à la protection des données et de la vie privée, Montréal (25 septembre 2007)	38

INTRODUCTION

Des centaines de personnes ont assisté à la 29^e Conférence internationale des commissaires à la protection des données et de la vie privée, qui s'est déroulée à Montréal du 25 au 28 septembre 2007. Intitulée « Terra Incognita » dans un esprit provocateur, la conférence s'articulait autour de thèmes concernant les rapports des anciens explorateurs avec des terres inconnues. S'inspirant du folklore selon lequel ces anciens explorateurs inscrivait régulièrement la phrase « here be dragons » sur les dessins illustrant les territoires non délimités¹, les organisateurs de la conférence ont classé les présentations en fonction de six « dragons » : la sécurité publique, la mondialisation, quand la loi rencontre la technologie, l'information ubiquiste, la prochaine génération et le corps humain comme donnée. Les réponses à ces « dragons » étaient décrites de diverses manières, alors qu'on parlait tantôt de « tueurs de dragons », de « dompteurs de dragons » et de « coalition contre les dragons ». Au nombre des mesures proposées, mentionnons la collaboration multisectorielle et intergouvernementale, les sceaux de confidentialité, la dépersonnalisation, les vérifications et les évaluations des facteurs relatifs à la vie privée (ÉFVP).

On rappelait régulièrement aux participants de la conférence qu'il ne restait que quelques minutes avant l'heure de l'entrée en scène de la société de surveillance totale, symbolisée par l'horloge de la société de surveillance de l'Union américaine pour les libertés civiles (ACLU)². Certains membres du milieu de la protection de la vie privée attribuaient la gravité de la situation actuelle aux percées limitées qu'on avait réalisées en matière de création de politiques qui préconisent la protection de la vie privée et au peu de succès avec lequel on avait su, de façon plus générale, gagner à la cause le cœur et l'esprit du public. La collaboration entre les secteurs, les groupes d'intervenants et les administrations territoriales était une pièce maîtresse évoquée dans la plupart des séances. Les projets centraux établis dans le cadre des initiatives de collaboration visaient notamment à repenser le sens de la protection de la vie privée, à éliminer la dichotomie entre vie privée et sécurité et à résoudre les incohérences dans les approches juridiques existantes, en se concentrant sur la durée de vie limitée des modèles de « consentement », « contrôle » et « propriété » des données qui ont présentement cours.

La partie I met en lumière certaines des choses que nous avons apprises sur les « dragons » lors de la conférence en ce qui concerne la mondialisation (y compris le

¹ En dépit du folklore, il semble qu'un seul explorateur aurait écrit une fois « here be dragons » (ici résident les dragons) sur une carte. Inscrit près de la côte est de l'Asie sur le globe Lenox vers 1503 (présentement exposé à la bibliothèque publique de New York) se trouve la phrase « Hc svnt dracones ». Même si des références aux animaux, y compris les dragons imaginaires, apparaissent sur d'autres cartes historiques, il semble que l'expression « here be dragons » n'ait été trouvée qu'une seule fois. En outre, certains ont associé cette phrase à l'expression utilisée par Marco Polo en lien avec certaines parties de l'Asie — le royaume de Dagoian — plutôt qu'au terme « dragon »: MapHist, « Where be Here Be Dragons? », en ligne : <http://www.maphist.nl/index.html>.

² Le 17 septembre 2007, l'ACLU a lancé l'horloge de la société de surveillance (Surveillance Society Clock) pour illustrer que nous nous rapprochons dangereusement d'une société de surveillance totale aux États-Unis. L'horloge indique qu'il ne reste que six minutes avant minuit, à savoir l'heure de la fin de la protection de la vie privée. ACLU, « ACLU Sets New "Surveillance Society Clock" at Six Minutes Before Midnight » (17 septembre 2007), en ligne : <http://www.aclu.org/privacy/gen/31852prs20070917.html>.

programme en matière de sécurité), la technologie (forage de données, identification par radiofréquence, repérage géodépendant, génétique et mise en banque de substances biologiques, informatique ubiquiste, nanotechnologie et établissement de normes), les générations futures et les crimes sur Internet. La partie II porte sur les trousseaux d'outils proposées pour tuer ou dompter les dragons, ou pour former une coalition contre eux (incluant la collaboration multisectorielle et intergouvernementale, les sceaux de confidentialité, la dépersonnalisation, les vérifications et les ÉFVP). La partie III nous fait passer de dossiers particuliers à des thèmes plus généraux abordés tout au long de la conférence, où l'on lève le voile sur d'importantes préoccupations qui offrent matière à réflexion pour l'avenir (sens de la protection de la vie privée, dichotomie entre vie privée et sécurité, et incohérences dans les approches juridiques existantes).

I. LES DRAGONS

Les dragons évoqués durant la conférence se répartissent grosso modo en quatre catégories : a) mondialisation; b) technologie; c) prochaine génération; d) crime sur Internet. Cela dit, nous avons abordé dans chacune des catégories de nombreuses questions et préoccupations.

A. Mondialisation

Les préoccupations liées à la sécurité et à la circulation continue de données entre les gouvernements transcendent les frontières territoriales en cette époque de mondialisation. Ces nouvelles conditions mondiales font appel à des solutions aptes à protéger la vie privée de nature non territoriale ou, à tout le moins, fondées sur une collaboration entre les autorités des divisions territoriales. Cependant, une telle collaboration n'est pas sans défis compte tenu du fait que les représentants assis à la table proviennent de nations ayant des cultures et valeurs différentes, et qu'ils s'efforcent d'élaborer des outils pour dompter (sinon tuer) des dragons pour qui les frontières n'ont aucun sens.

(i) Sécurité publique³

Dans le discours liminaire de la conférence, Michael Chertoff, secrétaire du département de la Sécurité intérieure (États-Unis), a évoqué le fait que les organismes d'application de la loi exigeraient de plus en plus l'accès aux renseignements personnels et la rétention de tels renseignements comme outil nécessaire pour assurer la sécurité publique. Le secrétaire Chertoff a brossé un tableau de la menace terroriste à laquelle est constamment soumise la sécurité publique et des besoins concomitants : analyse préliminaire par le gouvernement américain du dossier passager (DP) de tous les voyageurs sur des vols qui ont quitté des pays étrangers en destination des États-Unis⁴; détention par le

³ Le contenu de cette section est tiré des séances suivantes de la conférence : Michael Chertoff, discours liminaire, 26 septembre 2007; Barry Steinhardt, première séance plénière, « Dragons : La sécurité publique et la mondialisation » (26 septembre 2007)

(http://www.privacyconference2007.gc.ca/workbooks/pres_plenary1_01_f.ppt#268,1,Slide 1); Bruce Schneier, première séance plénière, « Dragons : La sécurité publique et la mondialisation » (26 septembre 2007) et Michael Geist, plénière de clôture (28 septembre 2007).

⁴ Le dossier passager comprend des renseignements tels que le nom, l'adresse, le numéro de téléphone ainsi que des renseignements sur le vol et le mode de paiement pour tous les passagers d'un vol aérien. Pour les

gouvernement américain d'un organe d'archivage d'empreintes digitales à 10 chiffres pour tous les non-Canadiens et non-Américains qui franchissent les points d'entrée des États-Unis; acceptation d'un nombre réduit de documents d'identification plus sécuritaires de la part des personnes qui se présentent elles-mêmes aux frontières américaines. Faisant valoir que l'analyse préliminaire des arrivants par le truchement de l'examen du DP réduisait de façon générale les atteintes à la vie privée puisque cette approche ciblait des personnes en particulier pour les soumettre à un interrogatoire secondaire, le secrétaire Chertoff en a déduit que la dichotomie entre la vie privée et la sécurité était en fait une fausse dichotomie.

Plusieurs présentateurs se sont penchés sur l'élargissement de la surveillance de l'État au nom de la sécurité publique, mais aucun n'a sans doute illustré son propos sous un angle aussi géographique que ne l'a fait le secrétaire Chertoff dans ses remarques, que Michael Geist a judicieusement assimilées, dans son discours de clôture, au jeté du gant par le milieu de la sécurité. Des conférenciers tels que Barry Steinhardt de l'ACLU ont exprimé leurs craintes quant à la bonne volonté et à la capacité du milieu de la sécurité américain de mettre en œuvre de manière équitable des systèmes tels que le DP. En outre, Steinhardt tout comme Bruce Schneier se sont dits inquiets de l'absence de preuve selon lesquelles les concessions en matière de protection de la vie privée engendrent véritablement une plus grande sécurité publique⁵. Soucieux de la protection des renseignements personnels des passagers dans les transports internationaux, les commissaires à la protection des données et de la vie privée de la conférence ont diffusé une « Résolution sur l'urgence d'établir des normes mondiales visant la protection des données des passagers dont se serviront les gouvernements pour appliquer les lois et assurer la sécurité frontalière »⁶.

(ii) Circulation et miroitage de données d'une frontière à l'autre⁷

La circulation continue de données entre les frontières, qui découle des modèles des entreprises privées conçus pour abaisser les coûts et offrir un service ininterrompu et multilingue à la clientèle, s'ajoute aux menaces à la vie privée que pose le plan d'action en matière de sécurité poursuivi par des intervenants gouvernementaux du monde entier. Comme les entreprises impartissent à des administrations dans le monde entier divers aspects de la collecte, de l'entreposage et de l'analyse des données, les anciens modèles axés sur la communication complète des renseignements aux clients et sur l'obtention de leur consentement à ces types de transactions deviennent de plus en plus périmés. Et puisque les diverses administrations en cause ont des lois, des us et coutumes et des approches divergentes en ce qui a trait à la protection des renseignements personnels, on ne peut pratiquement pas éviter une situation où les sources de données vivant dans un

vols à destination des États-Unis, cette information est transmise au département de la Sécurité intérieure, qui fait une analyse préliminaire de l'information afin de déterminer les passagers qui doivent être détenus pour un interrogatoire secondaire à leur arrivée aux États-Unis.

⁵ Steinhardt, note 3 ci-dessus; Schneier, note 3 ci-dessus.

⁶ Pour le libellé complet de la Résolution, voir l'annexe A.

⁷ Le contenu de cette section est tiré de la séance d'information de la conférence intitulée « Dragon : La mondialisation – La circulation et le miroitage de données » (26 septembre 2007), conférenciers : Martin Abrams (http://www.privacyconference2007.gc.ca/workbooks/pres_infosession1_01_f.ppt - 280,1,Slide 1), Benjamin Hayes et David Loukidelis.

secteur auront, à l'égard de la protection de la vie privée, des attentes différentes de ceux qui vivent en prédominance dans le secteur où les données sont stockées et manipulées. En outre, ces circulations transfrontalières de données démontrent la mesure dans laquelle la réglementation territoriale en matière de protection de la vie privée devient rapidement inefficace. Dans un tel contexte, la coopération entre les autorités de réglementation de différentes administrations géographiques et la conception de mécanismes permettant aux entreprises d'élaborer des normes uniformes, comme le cadre de protection de la vie privée de la Coopération économique de la zone Asie-Pacifique (APEC) (sujet abordé en détail dans la partie II(A)(i) ci-dessous), sont de plus en plus pertinentes.

(iii) Difficultés intergouvernementales⁸

La fluidité avec laquelle les données et l'information circulent entre les frontières nécessite une coopération intergouvernementale en ce qui concerne l'établissement de normes, la coopération en matière d'application des lois et les activités de relations publiques. Les efforts conjoints tels que les initiatives de l'OCDE sur l'application transfrontalière des lois relatives à la protection de la vie privée (dont on discute en détail dans la partie II (A)(i) ci-dessous) se sont de plus en plus fait sentir ces dernières années. Cela dit, il reste encore des pierres d'achoppement. Les limites posées aux initiatives conjointes efficaces incluent le manque de pouvoirs accordés aux commissaires à la protection des données et de la vie privée ainsi que l'existence de disparités culturelles marquées. Comme l'a décrit le commissaire Kohnstamm des Pays-Bas, ces disparités culturelles engendrent en certaines occasions des situations d'ignorance mutuelle, de soupçon et de sentiment de supériorité, lesquelles ne favorisent pas des relations de travail efficaces entre les administrations⁹. Les différences culturelles peuvent inclure la mesure dans laquelle les citoyens ont confiance en l'État, la question de savoir si le système est axé sur la prévention ou le dédommagement, et la mesure dans laquelle chaque administration démontre du respect envers les ressortissants étrangers. Pour en arriver à une collaboration efficace entre les nations, il est essentiel que les nations partenaires manifestent un engagement clair à traiter le droit à la vie privée et les intérêts des ressortissants de manière compatible avec la façon dont elles traitent leurs propres citoyens.

Durant toute la conférence, on a fait état de la nécessité d'une collaboration intergouvernementale et multisectorielle de même que des défis inhérents à un projet du genre. Les séances portant sur les croisements entre la loi et la technologie ont sans doute été celles où cette question a été le plus souvent évoquée.

⁸ Le contenu de cette section est tiré des séances suivantes de la conférence : Jacob Kohnstamm, première séance plénière « Dragons : La sécurité publique et la mondialisation » (26 septembre 2007); troisième atelier « Parcourir les quatre coins de la terre » (27 septembre 2007), conférenciers : Peter Schaar, Michael Donohue, Gus Hosein, Peter Hustinx et Colin Minihan (http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop3_02_f.ppt#268,1,Slide 1).

⁹ Kohnstamm, *ibid*, voir diapositive en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_plenary1_01_f.ppt#267,2, Ignorance mutuelle, soupçons et sentiment de supériorité.

B. Technologie

La technologie progresse souvent sans égard à la « loi » ou à d'autres mécanismes délimitant les valeurs et principes sociaux, et sans rapports avec ceux-ci. Sous bien des angles, la loi a été perçue jusqu'ici comme un obstacle au progrès étant donné qu'on y a recours pour faire en sorte que le développement soit compatible avec les principes établis, y compris ceux ayant trait à la protection de la vie privée, ce qui peut limiter le développement. Dans chacun des cas abordés lors de la conférence, qu'il s'agisse de forage de données, d'IRF, de repérage géodépendant, de mise en banque de substances biologiques, d'informatique ubiquiste ou de nanotechnologie, on constate que les autorités de réglementation juridiques s'efforcent de comprendre le sens social de la technologie et ses répercussions sur la société. La chose se constate dans les efforts pour prévoir les conséquences des développements imminents et dans les tentatives pour moderniser les règles et concepts juridiques en tenant compte des développements déjà survenus. Encore une fois, il semble que la collaboration sera un facteur déterminant pour résoudre ces questions. Bien que la collaboration entre les autorités de réglementation et les concepteurs de technologie semble à la fois possible et essentielle si l'on veut parvenir à intégrer la protection de la vie privée aux spécifications des projets de technologie¹⁰, il semble nécessaire de poursuivre le travail pour s'assurer de bien mettre à profit ces possibilités. L'établissement de normes figure parmi ces possibilités, comme permet de le constater la discussion dans la sous-partie (vii) ci-dessous.

(i) Forage de données¹¹

Le forage de données peut prendre place dans bon nombre de contextes et pour bien des raisons, y compris l'établissement de profils de marchés, les soins de santé et la surveillance de l'État. Toutefois, abstraction faite du contexte, le forage de données soulève des préoccupations en matière de protection de la vie privée puisqu'il implique l'utilisation secondaire de données recueillies au départ dans un contexte différent. Notre évaluation de l'exercice de forage de données est influencée par notre évaluation de la mesure dans laquelle la réutilisation des données en question empiète sur la vie privée et des avantages sociaux qui, croyons-nous, peuvent découler de l'utilisation secondaire des données dans un contexte particulier. Par conséquent, certains participants de la conférence ont fait valoir que l'utilisation secondaire de données reliées à la santé dans le cadre de la recherche médicale doit faire l'objet d'une évaluation différente de celle du forage de données exécuté à des fins telles que l'établissement de profils de marchés et la surveillance de l'État.

L'exemple de la surveillance de l'État, dont il a été question lors d'une séance, provenait du programme américain de sensibilisation à l'information sur le terrorisme (auparavant connu sous le nom de programme de sensibilisation à l'information totale). En vertu de

¹⁰ Pour de plus amples renseignements sur le concept d'intégration de la protection de la vie privée aux technologies, voir Ann Cavoukian, « Privacy by Design: A Crucial Design Principle » (17 septembre 2007), en ligne : http://www.ipc.on.ca/images/Resources/up-2007_09_17_UofT.pdf.

¹¹ Le contenu de cette section est tiré de la séance d'information de la conférence intitulée « Le forage des données » (28 septembre 2007), conférenciers : Philippa Lawson, Peter Fleischer, Bradley Malin et Richard Rosenberg (http://www.privacyconference2007.gc.ca/workbooks/pres_infosession1_03_f.ppt).

ce programme, les autorités américaines ont compilé des données d'une multitude de sources pour soi-disant débusquer à l'avance les personnes susceptibles de commettre des actes terroristes. Toutefois, au moins une étude a fait valoir que de tels actes sont si peu fréquents et les caractéristiques de chacune des attaques tellement uniques, qu'il était peu probable que les ressources investies dans ce type de modèle procurent une plus grande sécurité¹².

On a donné à entendre que le forage de données était particulièrement inquiétant dans les contextes où les sources de données n'étaient pas au fait du type de renseignements recueillis à leur propos, ni des fins auxquelles allaient servir ces renseignements. Entre autres solutions proposées devant ces préoccupations, il y a celle qui voudrait qu'on exige une communication accrue et constante de la part des responsables de la collecte de données et des utilisateurs, et celle impliquant l'élaboration de techniques pour rendre les données anonymes afin de réduire les risques qu'elles ne permettent de retrouver l'identité d'une personne en particulier¹³.

Par ailleurs, la définition et l'administration du concept du consentement éclairé posent un défi grandissant étant donné qu'il est si souvent difficile d'expliquer aux personnes concernées les modes de collecte, de rétention et d'utilisation des données. Qui plus est, d'autres préoccupations sociales découlent de la collecte et de l'utilisation secondaire des données à des fins d'établissement de profils, que ce soit dans le contexte du marketing privé, des soins de santé ou de la surveillance publique, toutes choses pouvant soulever de graves questions quant à savoir si l'on peut en toute légitimité aborder la pratique du forage même des données en s'appuyant sur un modèle de consentement individuel. Ces questions font l'objet d'une discussion poussée dans la partie III (C)(i) ci-dessous.

(ii) Identification par radiofréquence (IRF)¹⁴

La technologie d'IRF permet de repérer une étiquette ou une micropuce passive insérée dans un objet ou une personne. Même dans son application populaire courante à des fins de contrôle des stocks dans le secteur de la vente au détail, l'IRF permet dans une certaine mesure de repérer subrepticement les déplacements du produit, et ce faisant, des personnes liées à ce produit. Alors que l'avenir qui se dessine est celui de l'étiquetage des articles, nous nous rapprochons de la création d'une infrastructure d'informatique ubiquiste, dont nous discutons plus loin dans la sous-partie (v). Les préoccupations découlant des conséquences de l'IRF pour la vie privée ont attiré l'attention des commissaires à la protection des données et de la vie privée à l'échelle internationale¹⁵ et

¹² Voir par exemple l'exposé de Richard Rosenberg lors de la séance d'information « Le forage des données » (28 septembre 2007), en ligne :

http://www.privacyconference2007.gc.ca/workbooks/pres_infosession1_03_f.ppt#289,13, Les conséquences du forage des données sur la protection de la vie privée dans les secteurs public et privé.

¹³ Les faibles possibilités de « dépersonnalisation » complète des données ont été abordées dans le cadre d'une séance distincte décrite en détail dans la partie II(C) du présent document.

¹⁴ Le contenu de cette section est tiré de la séance d'information de la conférence sur l'IRF (26 septembre 2007), conférenciers : Stephen Lau, Katherine Albrecht, Laurent Bernat, Ann Cavoukian et Pankaj Sood, en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_infosession2_01_f.ppt.

¹⁵ Lors de la 23^e Conférence internationale des commissaires à la protection des données et de la vie privée à Sydney (Australie), les commissaires ont formulé une résolution sur la technologie de l'IRF

ont fait l'objet de directives émises en 2006 par le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario. Ces directives portaient sur des pratiques équitables en matière d'information¹⁶. Quoiqu'il en soit, les répercussions de l'IRF dans le contexte d'une structure d'information élargie, dans laquelle la collecte passive de données en temps réel concernant le mouvement peut être reliée à d'autres collectes de données, entraînent une remise en question des modèles existants axés sur la connaissance et le consentement des personnes concernées.

(iii) Repérage géodépendant¹⁷

Les conférenciers qui se sont exprimés sur le thème du repérage géodépendant ont examiné en profondeur les risques que la surveillance en temps réel pose à la vie privée. Il est possible de détecter les mouvements individuels grâce aux émissions d'information produites par divers dispositifs que transportent bon nombre d'entre nous, y compris les téléphones cellulaires. À l'heure actuelle, les compagnies de téléphones cellulaires recueillent des renseignements ayant trait à l'emplacement de leurs appareils auxquels ils fournissent des services plusieurs fois au cours d'une même heure. La situation soulève d'importantes questions quant à la nécessité de conserver ce type de données, quant à savoir à qui elles appartiennent et quant au caractère légitime des utilisations secondaires éventuelles. Parmi les autres applications possibles de ce système, mentionnons le repérage des employés, la publicité selon l'emplacement et la datation selon l'emplacement. D'autres dispositifs peuvent entrer en ligne de compte, notamment les systèmes mondiaux de localisation (GPS) et l'IRF qui permettent le repérage en temps réel des mouvements individuels. Les experts ont exprimé des inquiétudes du fait que, comme ces mécanismes de surveillance se combinent à d'autres données accessibles en ligne, un tel état de choses engendrera des systèmes de tri social et d'établissement de profils de plus en plus perfectionnés. L'assujettissement des personnes à l'« überveillance »¹⁸ nous privera graduellement de lieux publics dans lesquels nous pourrions évoluer sans crainte d'être jugés négativement. David Lyon a soulevé la préoccupation sociale plus générale selon laquelle on exploitera probablement ces systèmes de manière telle qu'ils isoleront davantage les personnes déjà marginalisées de notre société.

Le Groupe de travail sur l'ingénierie d'Internet (GTII) a élaboré la norme technique « GeoPriv », qui vise à protéger la vie privée dans des contextes où des renseignements

(20 novembre 2003), en ligne : http://www.cnil.fr/fileadmin/documents/uk/Resolution_RFID-VA.pdf. Voir également Commissariat à la protection de la vie privée du Canada, « Fiche d'information : L'identification par radiofréquence », en ligne : http://www.privcom.gc.ca/fs-fi/02_05_d_28_f.asp.

¹⁶ Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, « Privacy Guidelines for RFID Information Systems » (juin 2006), en ligne : <http://www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf>.

¹⁷ Le contenu de cette section est tiré du premier atelier de la conférence intitulé « Le système de repérage géodépendant » (26 septembre 2007), conférenciers : Alexander Dix, Éloïse Gratton, David Lyon, Michael Michael et John Morris

(http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop1_01_f.ppt#268,1, Slide 1).

¹⁸ Voir l'exposé de Michael Michael lors du premier atelier de la conférence intitulé « Le système de repérage géodépendant » (26 septembre 2007), diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop1_01_f.ppt#274,3, Überveillance: surveillance et repérage des gens – 24/7 x 365.

sur l'emplacement sont transmis en fonction des protocoles du GTII, y compris le protocole de voix sur IP¹⁹. La norme exige que des règles fondamentales de protection de la vie privée soient transmises en même temps que les données de localisation. Ces règles ont trait à la durée pendant laquelle on peut conserver les renseignements et aiguillent les intéressés vers des règles plus détaillées de protection des renseignements personnels stockés à l'externe. Bien que la norme rende possible la protection de la vie privée, sa mise en œuvre dépendra probablement d'une prescription juridique quant à l'application de cette norme. Cependant, on recense plusieurs cas où les décideurs politiques sont exhortés à plaider contre la mise en œuvre de telles caractéristiques de protection. Ainsi, des personnes ont fait valoir lors des audiences qui se sont déroulées aux États-Unis sur le 911 évolué que les gens ne devraient pas avoir la possibilité de désactiver le dispositif de localisation géographique sur leur téléphone cellulaire, car celui-ci peut empêcher de faire de faux appels au 911 ou accélérer les enquêtes concernant ces faux appels.²⁰

(iv) Génétique et mise en banque de substances biologiques²¹

La mise en banque de substances biologiques peut impliquer la collecte de renseignements extrêmement personnels ayant trait à la santé des personnes, ce qui soulève de graves préoccupations en matière de protection de la vie privée. Par ailleurs, l'accès à cette information est indispensable à la recherche sur la santé, au traitement clinique et aux analyses judiciaires. Dans certains cas, comme avec l'ADN, les données constituent des renseignements identifiables dont on peut difficilement éliminer les caractéristiques d'identification (ou qui peuvent être beaucoup moins utiles sans ces caractéristiques). Dans d'autres cas, comme celui de la génétique démographique, les données sont recueillies afin d'étudier les populations et il n'est pas nécessaire de les rattacher directement à des personnes identifiables. Ces deux types de situations soulèvent de nombreuses préoccupations liées à la protection de la vie privée.

Les données non dépersonnalisées peuvent révéler des aspects très personnels de la santé d'une personne qui pourraient servir de base de discrimination à moins d'exiger l'application étroite des mécanismes de contrôle d'accès à ces données et des utilisations qui en sont faites. La dépersonnalisation ou l'élimination de la possibilité de repersonnalisation peut compromettre la valeur clinique et informative des données utilisées à certaines fins, mais il semble également difficile de garantir de telles manœuvres étant donné que les percées technologiques sont un véritable terrain meuble en ce qui concerne les possibilités liées à la repersonnalisation.

¹⁹ Pour de plus amples échanges, voir « Geopriv Requirements », en ligne : <http://www.ietf.org/rfc/rfc3693.txt>.

²⁰ Voir l'exposé de John Morris lors du premier atelier de la conférence intitulé « Le système de repérage géodépendant » (26 septembre 2007), diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop1_01_f.ppt#297,26, Le combat pour la localisation : des préoccupations conflictuelles ne favorisent pas la protection de la vie privée ni l'innovation.

²¹ Le contenu de cette section est tiré du deuxième atelier de la conférence intitulé « La génétique et la mise en banque de substances biologiques », parties I et II (27 septembre 2007), conférenciers : Paul Chadwick, Bartha Maria Knopper, Timothy Caulfield, Martin Dufresne et William Lowrance (http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop2_02_f.ppt#256,1,Slide 1).

Bien que la collecte intergouvernementale de données puisse engendrer d'importants avantages, à savoir la création de bases de données dont on peut rapidement dériver des résultats valables reliés à la santé, des questions éthiques se posent quant à la vigueur du consentement obtenu des sources de données d'une administration à l'autre. L'un des mécanismes, qui est utilisé par des plates-formes de recherche comme celle du Québec, permet de mettre sur pied des bases de données de manière à pouvoir éliminer du système les données des personnes qui, à un moment donné, retirent leur consentement²².

En dépit de ces efforts, la mise en banque de substances biologiques soulève de sérieuses questions sur la viabilité continue d'un cadre conceptuel reposant sur les notions de consentement individuel et de propriété des renseignements — même dans le contexte de la recherche et des traitements en matière de santé. Un système qui porte sur l'obtention du consentement individuel, même s'il a été conçu pour réexaminer le contenu à toutes les fois où est faite une utilisation ultérieure des données, ne répond pas aisément aux préoccupations d'ordre social reliées aux utilisations secondaires des données en banque et à la possibilité d'établir des profils de groupe.

(v) Informatique ubiquiste²³

À mesure que les gens adoptent des technologies telles que les téléphones cellulaires, l'IRF et le GPS, notre monde est en train de devenir un lieu de diffusion de renseignements et de réseaux ad hoc puisque nos dispositifs transmettent des données à notre sujet et font une recherche de données sur d'autres personnes dans le voisinage. Ces poignées de main électroniques invisibles peuvent accélérer, simplifier et faciliter les transactions des uns avec les autres. À titre d'exemple, des gens peuvent trouver avantageux d'être ciblé par la publicité d'articles qui les intéressent dans des magasins de vente au détail alors qu'ils passent devant ce magasin, et ils peuvent trouver commode de pouvoir plus facilement et automatiquement localiser les gens qui leur sont chers lorsqu'ils sont loin de leur domicile. Les spécialistes du marketing comprennent également de façon claire les avantages du marketing ciblé sur l'emplacement.

Toutefois, ce monde de diffusion et de réception de renseignements soulève de lourdes appréhensions en matière de protection de la vie privée. Sera-t-il possible pour les gens de profiter de l'informatique ubiquiste sans compromettre complètement le caractère privé de leurs propres données? Il existe à cette question une réponse d'ordre technologique, à savoir le système individuel de protection des renseignements personnels (SIPRP). Les gens pourraient utiliser leur SIPRP pour mettre en banque leurs données personnelles et leurs transactions, mais seraient également en mesure de fixer le dispositif de manière à limiter l'accès des autres à ces données. À titre d'exemple, une personne pourrait ajuster son SIPRP afin qu'il fasse la distinction entre le forage de données par les spécialistes du marketing de détail et les demandes d'information par les

²² Voir l'exposé de Bartha Maria Knoppers lors du deuxième atelier de la conférence intitulé « La génétique et la mise en banque de substances biologiques » (27 septembre 2007), diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop2_02_f.ppt#359,23, Slide 23.

²³ Le contenu de cette section est tiré de la première séance plénière de la conférence intitulée « Dragon : L'informatique ubiquiste » (27 septembre 2007), conférenciers : Stephanie Perrin, Ian Kerr, Teresa Lunt, David Phillips (http://www.privacyconference2007.gc.ca/workbooks/pres_plenary1_02_f.ppt#363,1, Slide 1).

membres de sa famille. On pourrait également, pour mieux protéger la vie privée, programmer le dispositif de manière à ce qu'il indique à son propriétaire s'il court le risque de diffuser de l'information qui permettrait de l'identifier.

L'informatique ubiquiste entraîne également une remise en question des cadres juridiques entourant la protection des renseignements personnels. Théoriquement, le Canada a toujours structuré ses lois de manière hiérarchique en ce qui concerne les intérêts de nature privée, l'échelon le plus élevé à ce chapitre étant accordé au corps, et les échelons inférieurs aux emplacements et ensuite à l'information. Dans un monde d'informatique ubiquiste où les dispositifs se trouvant sur nos corps (ou, encore, nos corps eux-mêmes) transmettent des données à notre sujet alors que nous passons d'un endroit à l'autre, ces catégories deviennent de plus en plus floues. Dans la mesure où les intérêts de nature privée en cause sont principalement analysés comme étant d'ordre informatif, nous risquons d'assister à un rétrécissement inédit du niveau de protection de la vie privée offert par le droit canadien.

Le monde de l'informatique ubiquiste pourrait favoriser l'élaboration de lois qui s'écartent des notions de propriété individuelle, selon lesquelles la protection de la vie privée s'articule autour des choix d'une personne quant au contrôle de « ses » données. Au lieu de simplement intégrer la protection de la vie privée dans le concept technologique, l'informatique ubiquiste au Canada nous pousse à modifier nos conceptions existantes à l'égard de la protection de la vie privée. L'un des aspects de cette modification nous amènera à réfléchir non seulement aux manières dont les gens peuvent contrôler l'accès aux renseignements qui les identifient et l'utilisation qui sera faite de ces renseignements, mais aussi à l'agrégation de renseignements d'identification non personnels qui servent à créer des cadres culturels touchant les particuliers et les groupes dans la société. L'approche européenne en matière de protection de la vie privée comme droit fondamental de la personne offre un excellent guide dans ce processus de réflexion.

(vi) Nanotechnologie²⁴

La nanoscience implique du travail avec les atomes, donc avec la matière. L'une des caractéristiques importantes de la nanoscience est que les propriétés de la matière, comme la façon dont les atomes se déplacent et la vitesse de leur mouvement, changent lorsqu'on atteint un certain niveau de minutie. Ainsi, il est difficile de prédire la façon dont la nature et le comportement de la matière se modifiera sur l'échelle nanométrique, à savoir le niveau d'atomes dans la matière. Être capable de manipuler la matière au niveau atomique ouvre des possibilités de création de nouveaux types de structures et d'êtres.

La nanotechnologie implique la conception, la caractérisation, la production et l'application de structures. La nanotechnologie se trouve dans la phase de recherche et de

²⁴ Le contenu de cette section est tiré de la deuxième séance plénière de la conférence intitulée « La nanotechnologie et la protection de la vie privée » (26 septembre 2007), conférenciers : Jacques Saint-Laurent, Alex Türk, Hervé Fischer, Joel Reidenberg, Bernard Sinclair-Desgagné et de la séance d'information intitulée « Nanotechnologie II » (28 septembre 2007), conférenciers : Yves Poullett et Peter Grutter (http://www.privacyconference2007.gc.ca/workbooks/pres_infosession2_03_f.ppt).

découverte, ce qui est attribuable en partie aux coûts prohibitifs liés aux activités à l'échelle nanométrique. En plus d'offrir la possibilité de hausses exponentielles de capacité de stockage et de vitesse de calcul, les nanotechnologies peuvent soulever des questions bioéthiques en ce sens qu'elles peuvent nous permettre de recueillir et d'examiner des données sur les personnes au niveau de l'atome.

Les répercussions sur la protection de la vie privée associées à une capacité accrue de contrôler la matière à l'échelle nanométrique pourraient être énormes : le repérage passif simplifié à l'insu d'une personne et l'implication de citoyens dans une surveillance sans cesse importune d'autres citoyens ne représentant que deux de ces répercussions. Certains défenseurs des aspects juridiques et privés ont fait valoir lors de la conférence la nécessité de moderniser les instruments réglementaires et d'élaborer une convention internationale visant à intégrer les principes de protection de la vie privée dans le développement de la nanotechnologie. Ils sont d'avis que cette approche est préférable à celle où les autorités de réglementation sur la protection des renseignements personnels se contentent de réagir aux nanotechnologies développées séparément par des établissements privés. Comme pour bon nombre d'autres technologies abordées lors de la conférence, un aspect supplémentaire du défi qui se pose aux autorités de réglementation d'aujourd'hui est lié au fait de ne pas savoir en quoi consisteront les applications de demain.

(vii) Établissement de normes²⁵

L'établissement de normes fournit une occasion de mettre en branle le type de collaboration multisectorielle entre le milieu de la protection de la vie privée et les technologues suggérée dans le contexte de l'IRF, de la nanotechnologie et de l'informatique ubiquiste. De nouvelles technologies voient le jour en conformité avec des normes techniques établies en grande partie par les membres du milieu technologique. Au sein de cette collectivité, c'est surtout la Commission électrotechnique internationale (CEI) qui fixe les normes pour le matériel, tandis que l'Organisation internationale de normalisation (ISO) établit en grande partie les normes pour les logiciels. On a mis sur pied un comité technique conjoint pour combler l'écart entre ces deux organes de normalisation. En temps normal, le processus d'élaboration s'étire sur une période de 6 à 12 mois à la suite de laquelle les normes sont publiées et mises en œuvre. Le dialogue entre les intervenants du milieu de la protection de la vie privée et les technologues durant cette période est essentiel pour s'assurer que les principes de protection de la vie privée sont pris en compte dans la conception et la mise en œuvre des technologies.

Ces dernières années, on a constaté l'amorce de ces types de dialogue entre certains intervenants du milieu de la protection de la vie privée et les technologues.

L'International Security, Trust and Privacy Alliance (ISTPA), composée de divers établissements et technologues, a travaillé à l'élaboration d'un cadre technique pour les systèmes de technologie de l'information qui opérationnalise les principes de protection de la vie privée découlant de plusieurs sources de réglementation. La Résolution de la

²⁵ Le contenu de cette section est tiré du deuxième atelier de la conférence intitulé « Les normes », parties I et II (26 septembre 2007), conférenciers : John Borking, Colin Bennett, John Hopkinson, et John Sabo (http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop2_01_f.ppt).

Pologne en 2004²⁶, qui évoquait la nécessité d'établir une norme internationale de protection de la vie privée et qui définissait les principes du droit à la vie privée essentiels à l'élaboration de cette norme, a ouvert des possibilités de dialogue entre les commissaires à la protection des données et de la vie privée et les autorités de réglementation de l'industrie. L'adoption d'une seule norme offre la possibilité de déterminer si les engagements exprimés par diverses entreprises en matière de protection de la vie privée font effectivement l'objet d'une mise en œuvre.

C. Prochaine génération²⁷

Le monde en ligne forme une partie homogène de l'espace social des enfants et des adolescents. Certaines études antérieures sur les jeunes en ligne donnaient une vision relativement optimiste des enfants et des adolescents dans le cyberspace. Toutefois, il est de plus en plus évident que les modèles opérationnels en ligne qui servent au forage de données concernant les adultes s'appliquent également aux espaces occupés en majeure partie par des enfants et adolescents. Bon nombre de sites Web ciblant les enfants recueillent des renseignements qui permettent d'identifier des personnes de même que d'autres données détaillées sur leurs préférences afin d'élaborer des profils qui permettront aux sites de mieux cibler le marché des enfants. Plusieurs facteurs tendent à limiter la supervision parentale des activités en ligne des enfants, notamment les politiques de confidentialité difficiles à comprendre qu'appliquent ces sites de même qu'un écart entre les générations qui, dans bien des cas, signifie que les enfants sont plus habiles et mieux informés en ce qui touche les technologies que ne le sont les adultes dans leur quotidien.

En outre, bien que les jeunes soient concernés par leur vie privée, ils ont tendance à la percevoir différemment des adultes. Leurs principales préoccupations quant à leurs activités en ligne visent surtout à garder les renseignements qui les concernent hors de portée des gens qu'ils connaissent. Ils peuvent considérer comme moins risquée la diffusion généralisée des images et des renseignements personnels sur le plan de leur vie privée que la communication de cette même information à leurs familles et amis, qui occupent l'espace réel. Par conséquent, nous constatons une tendance grandissante d'auto-exposition en ligne par des jeunes ainsi que la diffusion d'images et de renseignements par des jeunes concernant des pairs. Action Média est à préparer une étude sur les dossiers concernant la protection de la vie privée des jeunes et la plate-forme Facebook²⁸.

Dans un tel contexte, il est crucial d'établir une collaboration multisectorielle internationale pour sensibiliser les gens et imposer des limites aux pratiques trompeuses.

²⁶ *Privacy Commissioners Resolutions on proposed ISO privacy standard and PETTEP*, [2004] PLPR 49, en ligne : <http://www.austlii.edu.au/au/journals/PLPR/2004/49.html>.

²⁷ Le contenu de cette section est tiré de la deuxième séance plénière de la conférence intitulée « La protection en ligne de la vie privée des enfants » (27 septembre 2007), conférenciers : Francesco Pizzetti, Jacquelyn Burkell, Leslie Regan Shade et Valerie Steeves (http://www.privacyconference2007.gc.ca/workbooks/pres_plenary2_02_f.ppt#268,1,Slide 1).

²⁸ Leslie Regan Shade, « "It Just Sucks You In": Young Women's Use of Facebook », Leslie Regan Shade, rédigé pour Action Média, novembre 2007, en ligne : www.media-action-media.com.

L'Union européenne (UE) a pris part à une série de mesures pour résoudre ces préoccupations, parmi lesquelles on retrouve le Livre vert de 1997, son plan d'action de 1999 et la directive du Conseil de l'UE de 2005 sur une utilisation sécuritaire d'Internet²⁹. Des membres de la société civile ont également joué un rôle actif dans l'élaboration de projets éducatifs, dont certains sont décrits ci-dessous dans la partie II(A)iii.

D. Crimes sur Internet³⁰

La séance ayant pour thème la sécurité publique avait trait aux crimes commis sur Internet et mettait l'accent sur la violence familiale, le harcèlement criminel, la fraude et le vol en ligne.

Les technologies visant à mieux protéger la vie privée ont rempli un double rôle dans la violence familiale et le harcèlement. D'une part, des gens ont utilisé les technologies capables d'infiltrer la vie privée pour commettre des actes répréhensibles. Des contrevenants ont exploité les enregistreurs de frappe et les logiciels espions pour surveiller les habitudes informatiques des survivants à des actes répréhensibles. Dans certains cas, ils ont fait obstacle aux tentatives pour trouver des refuges ou d'autres sources d'aide. En outre, les harceleurs ont eu recours à des dispositifs de géolocalisation et à des données achetées auprès de courtiers de données sous de faux prétextes pour retrouver leurs victimes³¹.

D'autre part, les harceleurs ont mis à profit des technologies qui améliorent la protection de la vie privée, telles que le brouillage des appels (pour empêcher l'identification de l'appelant) de manière à ce que leurs victimes ne puissent filtrer leurs appels. Abstraction faite de ces cas, les mécanismes d'amélioration de la protection de la vie privée ont joué un rôle crucial en aidant certaines femmes à fuir un climat de violence. L'importance de préserver les renseignements personnels des survivantes qui ont trouvé protection dans des refuges est au cœur même de la loi américaine³² qui, entre autres choses, limite la collecte de renseignements personnels sur les survivantes ayant recours aux services sociaux et aux refuges.

Symantec recueille de l'information à l'échelle mondiale en ce qui concerne les menaces en ligne telles que la fraude et le vol. La compagnie utilise quelque deux millions de

²⁹ Pour voir et consulter ces diverses initiatives financées par l'Union européenne : Safer Internet, « Une longue histoire avant le lancement du "Safer Internet Plan" » (« Initiatives de l'UE »), en ligne : <http://www.sip-bench.org/sipbench.php?page=history&lang=fr>.

³⁰ Le contenu de cette section est tiré du deuxième atelier de la conférence intitulé « Le crime sur Internet », parties I et II (28 septembre 2007), conférenciers : Joel Winston, Cynthia Fraser et Dean Turner (http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop2_03_f.ppt#268,1,Slide 1).

³¹ Dans *Helen Remsburg, Administratrix of the Estate of Amy Lynn Boyer c. Docusearch Inc.* 2003 N.H. LEXIS; 816 A.2d 1001; 2003 N.H. LEXIS 17, la succession d'une femme tuée par un harceleur criminel a poursuivi le courtier en données qui a obtenu des renseignements de la victime par faux-semblant et les a vendus au meurtrier.

³² *Violence Against Women and Department of Justice Reauthorization Act of 2005*, (« *Violence Against Women Act* ») H.R. 3402-24, sec. 107, en ligne : http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h3402enr.txt.pdf.

comptes leurre (aussi appelés « pots de miel ») pour attirer et contrôler le pollupostage et les programmes d'hameçonnage qui ont pour objet d'infiltrer les comptes des utilisateurs, surtout dans le but d'extraire des données financières. Étant donné la valeur de l'information financière, comme les cartes de crédit et les données bancaires, les outils permettant des invasions de la vie privée sur Internet sont devenus une entreprise, avec des logiciels conçus pour les activités criminelles, tels que MPack, un outil développé par des spécialistes et offert sur le marché.

Les violations de la vie privée en ligne se déroulent maintenant par étapes, l'objectif étant d'infiltrer des sites Web fiables qui, à leur insu, transmettent des liens aux utilisateurs de ces sites. La première étape dans le processus d'infection d'un système au moyen de logiciels espions ou malveillants, tels que Nimba ou Blaster, est de trouver un emplacement sur le système. L'enregistreur de frappe ou le programme malveillant est alors installé au cours d'une attaque ultérieure. Le cheval de Troie est le principal type de code malveillant installé en Amérique du Nord. Une fois qu'un cheval de Troie a infiltré un système et est téléchargé par les utilisateurs qui accèdent à ce système, il enregistre des renseignements personnels.

Puisque les compagnies de services financiers risquent d'être les principales cibles de ces logiciels malveillants en raison des grandes quantités de données personnelles qu'elles conservent, il est crucial pour ces organisations d'avoir en place des politiques détaillées en matière de sécurité non seulement pour les ordinateurs, mais aussi pour les supports de données de tout genre, y compris les iPods et les téléphones cellulaires. Les fuites et les infiltrations qui touchent ces organisations peuvent avoir des conséquences négatives auprès de milliers de personnes (p. ex. la perte de données de l'entreprise TJ Maxx)³³.

II. TUEURS DE DRAGONS/DOMPTEURS DE DRAGONS/COALITION CONTRE LES DRAGONS

Dans pratiquement toutes les séances de la conférence, les participants ont discuté de la nécessité centrale d'établir une collaboration multisectorielle et intergouvernementale pour s'attaquer aux graves menaces posées à la vie privée dans un monde où les technologies informatiques et les mécanismes de surveillance se font de plus en plus omniprésents. Au nombre des initiatives plus particulières dont il a été question, mentionnons les sceaux de confidentialité, la dépersonnalisation, les vérifications et les évaluations des facteurs relatifs à la vie privée (ÉFVP).

³³ Pour les résultats de l'enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Commissariat à l'information et à la protection de la vie privée de l'Alberta concernant la brèche dans la protection des données de TJX, voir Communiqué, « La brèche dans la protection des données de TJX est attribuable à des mécanismes de sécurité inadéquats, selon les commissaires » (25 septembre 2007), en ligne : http://www.privcom.gc.ca/media/nr-c/2007/nr-c_070925_f.asp.

A. Collaboration multisectorielle et intergouvernementale

Il semble y avoir eu unanimité autour du fait que les défis posés à la protection de la vie privée par l'informatique de plus en plus omniprésente nécessitent la contribution de divers intervenants ainsi que la collaboration entre eux, ce qui inclut les commissaires à la protection des données et de la vie privée, les membres de la société civile, les entreprises et les utilisateurs partout dans le monde. On a présenté aux participants de la conférence une impressionnante collection d'initiatives et de techniques de divers secteurs.

(i) Initiatives de Londres en 2006, de l'APEC et de l'OCDE

Ces dernières années, on a enregistré une multiplication d'initiatives multilatérales visant à établir des principes en matière de protection de la vie privée ainsi qu'à encourager les gouvernements à unir leurs efforts pour faire appliquer les lois. Parmi les initiatives clés mentionnées lors de la conférence, il y a celle de Londres en 2006, le Cadre de protection de la vie privée de l'APEC et les Lignes directrices de l'OCDE.

Lors de la 28^e Conférence internationale des commissaires à la protection des données et de la vie privée qui s'est déroulée à Londres en 2006, les participants ont appuyé ce que l'on connaît aujourd'hui sous le nom d'« Initiative de Londres ». Conformément à cette initiative, les commissaires ont convenu de ce qui suit :

- (i) coordonner leurs efforts pour élaborer des activités de communication sur la base d'idées communes;
- (ii) adapter leurs pratiques et méthodes de travail, grâce à l'évaluation de leur efficacité et au renforcement de leurs capacités d'expertise, de prospective et d'intervention dans le champ technologique;
- (iii) participer aux efforts pour faire reconnaître les autorités de protection des données (APD) par les institutions à l'échelle internationale, et promouvoir la participation d'autres intervenants nationaux et internationaux³⁴.

Par l'entremise de cette initiative, on reconnaît expressément la nécessité d'une collaboration intergouvernementale et multisectorielle, et on prend les mesures initiales pour rendre officielle sa mise en œuvre. Plusieurs manifestations précédentes illustrant ces types d'efforts ont fait l'objet de maintes discussions durant la conférence — particulièrement en ce qui concerne le cadre de protection de la vie privée de l'APEC et les Lignes directrices de l'OCDE.

Lors du Sommet de Sydney qui s'est tenu en juin 2007, 13 des 21 économies qui composent l'APEC ont accepté de participer à un projet exploratoire ayant trait à l'application transfrontalière des lois relatives à la protection des renseignements personnels. Ce projet découle de l'approbation ministérielle en 2004 du cadre de protection de la vie privée de l'APEC, qui cernait neuf principes de base ayant trait à la protection de la vie privée, notamment la responsabilisation, l'accès, la correction des

³⁴ Voir 28^e Conférence internationale des commissaires à la protection des données et de la vie privée, « Communiquer sur la protection des données et la rendre effective » (2006), en ligne : <http://ico.crl.uk.com/files/ComF.pdf>.

données, la sécurité et les mesures de sauvegarde³⁵. Les principaux objectifs du projet exploratoire sont au nombre de cinq : (i) promouvoir un cadre conceptuel de principes sur la façon dont les règles transfrontalières devraient fonctionner d'un pays à l'autre; (ii) promouvoir l'élaboration d'un processus consultatif sur la meilleure manière de mobiliser les intervenants; (iii) promouvoir l'élaboration de documents et de procédures pratiques, comme des formulaires d'auto-évaluation et des critères d'examen; (iv) analyser la façon de mettre en œuvre les divers documents et procédures; (v) promouvoir des activités de sensibilisation et de rayonnement³⁶. Outre le projet exploratoire, on insiste beaucoup sur l'éducation et la collaboration dans les initiatives de l'OCDE axées sur la protection de la vie privée³⁷. L'une des caractéristiques importantes de ces initiatives implique des efforts accrus sur la réduction des données plutôt que la seule utilisation et rétention des données.

(ii) Planification de la protection des renseignements personnels dans le travail de conception

Le concept de « planification de la protection des renseignements personnels dans le travail de conception » nous amène à faire fond sur le thème global de collaboration multisectorielle et intergouvernementale en insistant sur la nécessité d'une interaction entre les entreprises, les technologues et les autorités de réglementation relatives à la protection des renseignements personnels. Lors de la conférence, divers présentateurs ont mis en lumière plusieurs exemples de ces types d'initiatives. Des membres du milieu de la protection de la vie privée ont participé à des initiatives d'établissement de normes techniques telles que l'analyse des principes de la protection de la vie privée de l'ISTPA et la Résolution de la Pologne prise en 2004³⁸. Entre autres initiatives provenant du milieu même de la protection de la vie privée, mentionnons l'élaboration des normes GeoPriv³⁹ et la recherche ayant trait au développement d'appareils pour protéger la vie privée⁴⁰, les deux visant à donner aux gens un degré de contrôle accru sur la diffusion de données liées aux technologies fondées sur l'emplacement. Au nombre des récentes initiatives proactives lancées par les autorités de réglementation sur la protection de la vie privée et des données, mentionnons la diffusion de lignes directrices sur la protection de la vie privée ayant trait à l'IRF et aux principes de planification de la protection des renseignements dans le travail de conception (principes rédigés par le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario⁴¹).

³⁵ APEC, « APEC Privacy Framework Principles » (2005), en ligne : [http://www.ministerjusticeandcustoms.gov.au/www/agd/rwpattach.nsf/VAP/\(03995EABC73F94816C2AF4AA2645824B\)~APEC+Privacy+Framework.pdf/\\$file/APEC+Privacy+Framework.pdf](http://www.ministerjusticeandcustoms.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf).

³⁶ Malcolm Crompton, « The APEC Privacy Framework: Creating Trust in Developing Cross-Border Privacy Rules: A Progress Report » (mars 2007), en ligne : <http://iispartners.com/apec8march.pdf>.

³⁷ Pour de plus amples discussions sur les initiatives de l'OCDE, voir Direction de la science, de la technologie et de l'industrie de l'OCDE, « L'application transfrontière des lois de protection de la vie privée », en ligne : http://www.oecd.org/document/25/0,3343,fr_2649_34255_37572110_1_1_1_1,00.html.

³⁸ Voir « Les normes », parties I et II, note 25 ci-dessus.

³⁹ Voir « Le système de repérage géodépendant », parties I et II, note 17 ci-dessus.

⁴⁰ Voir l'exposé de Teresa Lunt, note 23 ci-dessus.

⁴¹ Voir le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, en ligne : <http://www.ipc.on.ca/index.asp?navid=58&layid=74&csid1=0&csid2=0&fid1=&fid2=5&fid3=&lang=2>.

(iii) Initiatives de la société civile⁴²

En parallèle avec la conférence, il s'est tenu le 25 septembre 2007 un forum spécial de la société civile, qui a engendré un document déposé devant les commissaires lors de la conférence. Son titre : Déclaration des organisations de la société civile sur le rôle des commissaires à la protection des données et de la vie privée⁴³. Les auteurs de la Déclaration recommandent, entre autres choses, d'élargir la mission des commissaires, d'accroître les efforts proactifs des commissaires pour encourager les gouvernements à ne pas abaisser les normes, et de donner suite aux préoccupations concernant le milieu de la sécurité et les services commerciaux. La Déclaration met l'accent sur la nécessité de prendre des mesures rapides et de fournir des efforts concertés pour empêcher qu'on ne surveille couramment les déplacements des gens.

L'une des principales préoccupations de la société civile est de réussir à mobiliser une section élargie de la population en ce qui concerne la protection de la vie privée. Les membres de la société civile sont invités à relever le défi posé par les menaces à la vie privée à plusieurs niveaux, notamment :

- en présentant des cas types aux commissaires et devant les tribunaux⁴⁴;
- en menant des campagnes d'éducation et de sensibilisation, c'est-à-dire :
 - organiser des manifestations politiques, notamment en exploitant des systèmes de réseautage sociaux en ligne pour susciter de l'intérêt et établir des communautés;
 - tenir les gouvernements et les organisations commerciales responsables du contrôle des activités et des atteintes liées à la vie privée⁴⁵;
 - mieux comprendre la façon dont les enfants et les adolescents évoluent dans l'environnement Internet et élaborer des mécanismes multimédias accessibles et faciles à comprendre pour communiquer avec les enfants

⁴² Le contenu de cette section est tiré du quatrième atelier de la conférence intitulé « Rapport sur l'atelier à l'intention de la société civile en matière de vie privée », parties I et II (27 septembre 2007), conférenciers : Barry Steinhardt, Ben Hayes, Roch Tassé et Ralf Bendrath (partie I) et Colin Bennett, Simon Davies, Alexander Dix, Barry Steinhardt et Jennifer Stoddart (partie II).

⁴³ Le libellé complet de la déclaration est joint à l'annexe B.

⁴⁴ Par exemple : *Lawson c. Accusearch Inc.*, [2007] A.C.F. n° 164 (conclut que la commissaire à la protection de la vie privée du Canada a compétence pour faire enquête sur une plainte de la directrice de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) au sujet d'une entreprise américaine qui aurait recueilli, utilisé et communiqué à des Canadiens des renseignements personnels concernant des Canadiens; Demande d'enquête adressée à la commissaire à la protection de la vie privée du Canada par la CIPPIC concernant Google Inc. et Double Click Inc. (17 septembre 2007), en ligne : http://www.democraticmedia.org/files/G-DC_Privacy_complaint_17Sept07.pdf.

⁴⁵ Voir par exemple « A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network », David Murakami Wood (dir. publ.) (septembre 2006), en ligne : http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf; Electronic Privacy Information Center and Privacy International, *The Privacy and Human Rights Report*, publié annuellement depuis 1997, en ligne : <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-545223>; The Surveillance Project, « Location Technologies: Mobility, Surveillance and Privacy » (mars 2005), en ligne : <http://www.queensu.ca/sociology/Surveillance/files/loctech.pdf>.

- et les adolescents en ce qui concerne les préoccupations que soulève Internet pour la vie privée⁴⁶;
- prendre en compte le travail que mènent les universités pour redéfinir les caractéristiques de la « nature » de la vie privée, en faisant valoir qu'il ne s'agit pas simplement d'un droit individuel contre la surveillance de l'État, et développer ainsi l'intérêt du public;
 - en effectuant des recherches sur les questions liées à la protection de la vie privée, parfois par le biais de financement fourni par les commissariats.

Les membres de la société civile tentent de maintenir un dialogue avec les commissaires à la protection des données et de la vie privée, notamment dans le cadre de conférences futures comme celle dont nous discutons dans le présent document.

B. Sceaux de confidentialité⁴⁷

Les sceaux de confidentialité représentent une marque de confiance envers des activités commerciales et signalent aux consommateurs la conformité de telles activités à certaines normes de protection de la vie privée. Les sceaux fournissent aux clients de l'information sur les pratiques de protection des renseignements personnels auxquelles ont recours les services qu'ils utilisent d'une manière moins compliquée et difficile à comprendre que ce qui apparaît en petits caractères dans une politique de confidentialité. Deux organisations, soit TrustE des États-Unis et PriSE de l'Allemagne, ont donné un aperçu du fonctionnement de leurs programmes en matière de sceaux de confidentialité.

TrustE fixe des normes de protection de la vie privée ayant pour but de répondre, à tout le moins, aux exigences juridiques des États-Unis. L'organisation vérifie le dossier des demandeurs afin de déterminer s'ils répondent à la norme. Ceux qui y répondent ont alors droit de recevoir un sceau de confidentialité qui représente une marque de confiance pour les consommateurs. TrustE contrôle les organisations qui ont reçu un tel sceau pour s'assurer qu'elles demeurent en conformité, et offre un mécanisme de plainte ainsi qu'un mode de règlement extrajudiciaire des différends pour résoudre les problèmes qui surgissent entre les détenteurs de sceaux et les consommateurs.

PriSE fait appel à des experts indépendants qui évaluent la conformité des demandeurs aux règlements sur la confidentialité et la sécurité de la technologie de l'information. Les experts produisent ensuite un rapport évalué par PriSE pour déterminer si le produit de

⁴⁶ Voir par exemple Réseau éducation-médias, « Jeunes Canadiens dans un monde branché » (2000-2005), en ligne : <http://www.media-awareness.ca/francais/recherche/JCMB/index.cfm>; Fédération canadienne des enseignantes et des enseignants, « Place aux jeunes dans les médias » (2004), en ligne : <http://www.ctf-fce.ca/f/resources/MERP/index.asp>. En ce qui concerne l'élaboration de cursus, voir <http://www.cybersmart.org/home/>; Centre de recherche sur les libertés civiles de l'Alberta, « Techno-tonomy: Privacy, Autonomy and Technology in a Networked World », en ligne : http://www.aclrc.com/techno_tonomy/index.html.

⁴⁷ Le contenu de cette section est tiré de la séance d'information de la conférence intitulée « À qui faites-vous confiance? Un regard sur les sceaux de confidentialité » (27 septembre 2007), conférenciers : Christine Varney, Kirsten Bock et Fran Maier, en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_infosession1_02_f.ppt.

l'organisation devrait recevoir le sceau de PriSE. Cette dernière a attribué 40 certifications depuis 2003. En 2007, elle a amorcé un projet à l'échelle de l'Europe qui regroupe des participants des secteurs privé et public. Le concept vise à permettre à des organisations de recevoir des sceaux valables à l'échelle locale ou dans toute l'Europe dans le cadre de projets pilotes au Royaume-Uni, en Slovaquie, en Autriche, en Espagne et en Suède. La certification a une durée de deux ans, renouvelable à l'échéance sous réserve de la réussite d'une évaluation ultérieure.

Les deux organisations reconnaissent qu'il y a risque d'utilisation frauduleuse des sceaux, et recherchent des mécanismes de vérification pour combattre ce problème.

C. Dépersonnalisation⁴⁸

La dépersonnalisation des données suppose la modification de ces données pour s'assurer qu'on ne peut les relier à une personne identifiable. Selon certains intervenants, les gens et les comités d'éthique de la recherche auraient moins de préoccupations en matière de protection de la vie privée s'il était impossible de relier les données pour identifier les personnes d'où proviennent ces données. D'autres intervenants estiment plutôt que la personnalisation n'est qu'une préoccupation parmi une foule d'autres découlant de la collecte, de l'utilisation et de la conservation des données. On a beaucoup discuté de la dépersonnalisation lors de la conférence dans le contexte des données reliées à la santé.

L'un des problèmes de base que pose la dépersonnalisation est l'absence d'un ensemble unique de connaissances heuristiques grâce auxquelles prédire si les données dépersonnalisées pourraient mener à la repersonnalisation de la personne à laquelle les données sont associées. Une grande partie dépend de la taille de l'ensemble de données et du mode d'attaque sur les bases de données contenant l'information. Selon une étude de Latanya Sweeney utilisant les données sommaires du recensement américain de 1990, 87 p. 100 des Américains ont déclaré des caractéristiques qui les rendaient identifiables en s'appuyant uniquement sur leur code postal, leur sexe et leur date de naissance⁴⁹.

En outre, les données dépersonnalisées regroupées sont moins valables dans de nombreux domaines de recherche médicale, particulièrement en génétique et en génomique. Même si nous extrayions les données génétiques contenues dans les éléments d'information autres que ceux nécessaires pour étudier une maladie ou une défectuosité particulière, nous pourrions découvrir plus tard qu'il est possible, dans les faits, de dégager d'autres renseignements à partir de ces données. Il a également été question lors de la conférence de nombreux mécanismes pour trouver un équilibre entre l'intérêt public envers la recherche sur la santé et les intérêts publics et privés envers la protection de la vie privée

⁴⁸ Le contenu de cette section est tiré du quatrième atelier de la conférence intitulé « Protéger la vie privée au moyen de la dépersonnalisation : réalité ou illusion? », parties I et II (27 septembre 2007), conférenciers : Ann Cavoukian, Khaled El Emam, William Lowrance, Bradley Malin, Donald Willison et Debra Grant, en ligne :

http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop4_01_f.ppt#268,1,Slide 1.

⁴⁹ L. Sweeney, « *k*-anonymity: a model for protecting privacy », *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, n° 5, 2002, p. 557–570, 558, en ligne : <http://privacy.cs.cmu.edu/people/sweeney/kanonymity.pdf>.

liée aux données et à l'information en matière de santé lorsque se présentent des situations telles que celles dont il a été question au cours de la conférence.

D'autres possibilités consistent à limiter le nombre de collectivités à qui sont communiquées les données, à accroître la surveillance indépendante de l'usage de l'information et/ou à en sanctionner l'utilisation malveillante, y compris en relation aux tentatives des intrus de repersonnaliser des données. Sans doute que la solution de rechange ayant attiré le plus d'attention consistait à trouver des mécanismes pour obtenir un consentement solide de la source de données, consentement qui prévoit la possibilité que différents types d'utilisation et de résultats ayant trait aux données surviennent dans l'avenir. Dans une publication récente, Willison et al.⁵⁰ faisaient la chronique d'une étude des comportements des patients envers l'utilisation de leurs données. Bien que les sujets ayant fait l'objet de l'enquête aient indiqué avoir une grande confiance envers les organismes qui recueillaient les données sur leur santé, la plupart auraient aimé avoir un mot à dire sur les utilisations qu'on allait faire de leurs données à l'avenir. Cet état de choses laisse entendre qu'on a besoin d'un mécanisme pour obtenir un consentement sur une base continue, plutôt que le modèle binaire actuel fondé sur l'obtention d'un consentement pour une utilisation particulière de données lorsqu'elles sont recueillies. Comme nous en discuterons en détail dans la partie III(c)(i) ci-dessous, certaines personnes ont cependant exprimé des inquiétudes devant une approche de ces enjeux axée sur le consentement individuel.

D. Vérifications⁵¹

Les vérifications axées sur la protection de la vie privée donnent l'occasion de contrôler régulièrement la conformité des organisations aux règlements et aux normes en matière de protection de la vie privée. Elles peuvent se dérouler sur un mode proactif ou en réaction à des plaintes. Les participants de la conférence ont discuté des systèmes de vérification tant privés que publics.

Le pouvoir que possèdent les commissaires à la protection des données et de la vie privée de vérifier la conformité aux règlements en matière de protection de la vie privée varie d'un pays à l'autre. Ceux de l'Espagne, du Royaume-Uni et du Canada disposent tous de pouvoirs de vérification, bien que ceux de la commissaire canadienne dépendent de la détermination de motifs valables. Les vérifications par les autorités de réglementation publique donnent l'occasion de promouvoir la conformité, de saines pratiques de protection des renseignements personnels et le dialogue avec des organismes éducatifs et privés.

⁵⁰ D.J. Willison, L. Schwartz, J. Abelson, C. Charles, M. Swinton, D. Northrup et L. Thabane, « Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public? », *Journal of the American Medical Information Association*, 2007, n° 14, p. 706–712, en ligne : <http://www.j-amia.org/cgi/content/abstract/14/6/706?ct>.

⁵¹ Le contenu de cette section est tiré du troisième atelier de la conférence intitulé « La vérification » (parties I et II), conférenciers : Artemi Lombarte, Yim Chan, Nicholas Cheung, Chris Turner et Joel Winston, en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop3_01_f.ppt#268,1,Slide 1.

À l'heure où la circulation transfrontalière des données devient un aspect de plus en plus courant des modèles des entreprises privées, les efforts concertés en matière de vérification entre les commissaires de différents gouvernements ont pris une importance renouvelée. Selon le contrat type de la Commission de l'UE de 2002 pour les transferts internationaux de données, un commissaire peut vérifier l'importateur de données issues d'une organisation que se trouve dans sa juridiction en utilisant les mêmes techniques et outils mis à la portée de ce commissaire en ce qui touche l'exportateur de ces données⁵². L'organisme espagnol de protection des données s'est inspiré de ce pouvoir pour mener une vérification de la sécurité et de l'utilisation des données exportées de l'Espagne vers la Colombie. L'exercice a permis de conclure qu'il y avait conformité générale⁵³.

Aux États-Unis, la Commission fédérale du commerce (FTC) réalise les fonctions de vérification, qui portent sur les pratiques inéquitables et trompeuses. La FTC poursuit une approche concertée, qui consiste notamment à vérifier les pratiques des organisations en matière de protection de la vie privée dans les cas où a été déposée une plainte d'illégalité (comme une pratique commerciale trompeuse). Au cours de ces enquêtes, la FTC a recours à des vérificateurs externes. Son approche est purement réactive dans un tel contexte, bien qu'elle consacre beaucoup de temps à des initiatives d'éducation pour tenter d'aider les organismes privés à élaborer et mettre en œuvre des politiques sur la protection de la vie privée.

Dans le secteur privé, l'Institut canadien des comptables agréés (ICCA) a élaboré pour les comptables des principes généralement reconnus en matière de protection des renseignements personnels, qui établissent une norme nord-américaine. Les 10 principes comprennent 60 critères mesurables établis pour permettre de réaliser une évaluation interne ou externe de la conformité des entreprises privées. Bien que les normes reflètent les prescriptions juridiques en Amérique du Nord, les principes ne sont pas conçus en vue d'une vérification de la conformité aux lois. IBM a élaboré son propre outil d'évaluation interne de la protection des renseignements personnels en regroupant des exigences axées sur la protection de la vie privée de partout dans le monde. Elle se sert ensuite de cet outil pour évaluer sa conformité à ces normes.

⁵² Voir Commission des Communautés européennes, Décision du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE (2001/497/CE), en ligne : http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2001/l_181/l_18120010704fr00190031.pdf.

⁵³ Artemo Lombarte, « Atelier sur la vérification en matière de protection de la vie privée : observations du président », présenté dans le cadre du troisième atelier de la conférence intitulé « La vérification » (27 septembre 2007), voir diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop3_01_f.ppt#269,2,Terra Incognita.

E. Évaluations des facteurs relatifs à la vie privée (ÉFVP)⁵⁴

Les ÉFVP ont pour but de s'assurer que les gouvernements évaluent et contrôlent la façon dont leurs initiatives et programmes agissent sur la vie privée des personnes. Les rapports découlant des ÉFVP peuvent servir à favoriser la transparence et donner des occasions de contrôler la conformité des organismes aux principes du droit à la vie privée.

Toutes les institutions fédérales figurant à l'annexe de la *Loi sur la protection des renseignements personnels*, exception faite de la Banque du Canada, doivent réaliser des ÉFVP en rapport avec les nouveaux programmes et services qui touchent la vie privée. Le Commissariat à la protection de la vie privée du Canada offre une consultation initiale, examine les ÉFVP et peut formuler des observations et des recommandations à cet égard. Le Commissariat a diffusé récemment un rapport de vérification de la conformité des ministères à la *Politique d'évaluation des facteurs relatifs à la vie privée* (ÉFVP)⁵⁵ et collabore activement avec les représentants du Conseil du Trésor qui travaillent à revoir leurs politiques afin d'améliorer le processus d'ÉFVP.

Les ÉFVP ne sont pas sans susciter des difficultés opérationnelles, au nombre desquelles figure un manque de ressources et d'expertise dans leur préparation et leur contrôle au sein des organismes gouvernementaux. Pour faire face à ce type d'enjeux, les participants de la conférence ont recommandé de mieux adapter les exigences à la taille et à l'ampleur des projets auxquelles elles s'appliquent, de donner des directives claires sur l'essence des ÉFVP et le rôle qu'elles sont censées remplir, et enfin de définir clairement les rôles et obligations des divers intervenants. Les gestionnaires du gouvernement chargés d'assurer la conformité doivent acquérir la formation et les connaissances spécialisées voulues pour comprendre les rapports des consultants, peu importe si un commissaire doit simplement examiner le rapport ou en faire l'approbation active. Le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario a mis sur pied un centre d'excellence en ÉFVP afin que le gouvernement puisse acquérir une expertise dans ce domaine⁵⁶.

On recense plusieurs facteurs cruciaux au fonctionnement efficace des ÉFVP. Celles-ci doivent permettre le traitement logique de sujets pertinents, et être complètes, précises et

⁵⁴ Le contenu de cette section est tiré du premier atelier de la conférence intitulé « L'évaluation des facteurs relatifs à la vie privée », parties I et II (27 septembre 2007), conférenciers : Blair Stewart, Claude Beaulé, LeRoy Brower, David Flaherty, Donald Lemieux, Rebecca Richards, Trevor Shaw, Blair Stewart, Mark Vale et Nigel Waters, en ligne :

http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop1_02_f.ppt.

⁵⁵ Rapport de vérification de la commissaire à la protection de la vie privée du Canada, « Évaluation des facteurs relatifs à la vie privée des programmes, plans et politiques », octobre 2007, en ligne :

http://www.privcom.gc.ca/information/pub/ar-vr/pia_200710_f.asp.

⁵⁶ Commissariat à l'information et à la protection de la vie privée de l'Ontario et département de la Justice des États-Unis, « Privacy Impact Assessment for Justice Systems » (2000), en ligne :

<http://www.ipc.on.ca/index.asp?layid=86&fid1=326>. Le Commissariat à la protection de la vie privée de l'Australie a également diffusé un guide en ligne sur les évaluations des facteurs relatifs à la vie privée :

« Privacy Impact Assessment Guide » (août 2006), en ligne :

<http://www.privacy.gov.au/publications/pia06/index.html>.

rédigées dans un langage clair. Il est indispensable de les fonder sur les prescriptions juridiques applicables, de les tenir à jour et d'en faire le contrôle. Le Commissariat à l'information du Royaume-Uni a distribué un manuel détaillé des ÉFVP lors de sa conférence sur la société de surveillance, le 11 décembre 2007⁵⁷.

III. THÈMES RÉCURRENTS

Certains thèmes ont été évoqués à répétition lors de la conférence, ce qui a permis d'établir des liens stratégiques et conceptuels importants sur la vaste liste de dragons et de tueurs de dragons recensés. En cette époque où la diffusion, la collecte, le stockage et le transfert des données semblent incessants, sans égard aux frontières, la question centrale des partenariats et efforts de collaboration multisectoriels et intergouvernementaux a été abordée dans presque toutes les séances. Alors que nous sommes aux prises avec les menaces posées à la protection de la vie privée dans ce nouveau monde, l'unanimité a semblé se faire sur le besoin d'amorcer un dialogue et d'établir une stratégie parmi les autorités de réglementation, les technologues, les membres de la société civile, les utilisateurs et les entreprises. L'engagement démontré par les commissaires de partout dans le monde envers la poursuite de cette vision de collaboration se constate à toutes les occasions, depuis l'Initiative de Londres en 2006 jusqu'au cadre de protection de la vie privée de l'APEC, en passant par le concept de planification de la protection des renseignements personnels dans le travail de conception, et l'inclusion des organismes de la société civile dans le dialogue et les conférences comme celle dont il est question dans le présent document.

Par contre, on avait un sentiment sans doute aussi fort que la collaboration n'est qu'un point de départ. Les représentants des intervenants de divers groupes ont réfléchi à l'importance de dégager des définitions communes de la protection de la vie privée, à la fois pour mieux interpeler le cœur et l'esprit du public ainsi que pour élaborer et mettre en œuvre des stratégies aptes à préserver les engagements centraux qui sous-tendent les mesures de protection de la vie privée. On a soulevé au moins trois types de questions conceptuelles à divers moments de la conférence, et ce, dans le cadre de plusieurs séances : (i) le sens de la protection de la vie privée; (ii) la dichotomie entre vie privée et sécurité; (iii) les incohérences dans les approches juridiques existantes au sein de certains gouvernements.

A. Le sens de la protection de la vie privée

Les participants de la conférence ont remis en question, à l'occasion de plusieurs séances, l'utilité de conceptualiser sous deux aspects la protection de la vie privée dans le sillage du nouvel environnement de l'informatique ubiquiste. Premièrement, nombre de participants ont fait valoir que la technologie allait probablement devancer la conception voulant que la vie privée se rapporte uniquement aux renseignements permettant d'identifier des personnes. Cette idée a été illustrée de manière graphique dans le cadre

⁵⁷ Commissariat à l'information du Royaume-Uni, « Surveillance Society Conference December 2007 », en ligne : http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_conference.aspx.

des discussions sur l'IRF, le repérage géodépendant, la génétique et la mise en banque de substances biologiques, ainsi que l'informatique ubiquiste. Dans un monde où les données circulent de manière limitée ou que l'accès à ces données est limité, nous pouvons trouver un certain soulagement dans l'idée que certaines données prises isolément ne permettent pas d'identifier une personne. Toutefois, comme nous l'avons mentionné plus tôt, l'étude de Sweeney a démontré que la réunion de seulement trois éléments de données (code postal, sexe et date de naissance) permet d'identifier 87 p. 100 des Américains⁵⁸. Alors que nous œuvrons dans un monde où les gens peuvent transporter des appareils d'où émanent des données, comme l'IRF, le GPS et les téléphones cellulaires, et où les technologies rendent possibles le stockage de quantités grandissantes de données et l'accès à ces données, il devient de plus en plus complexe de définir ce en quoi consiste les renseignements identifiables. Les données qui, aujourd'hui, ne semblent pas faire partie de ces renseignements, pourraient bien s'y retrouver demain, simplement en raison de nouvelles sources de données auxquelles elles seront combinées. La même préoccupation se fait entendre dans le contexte de la génétique et de la mise en banque de substances biologiques, où les données qui semblent dépersonnalisées aux fins poursuivies aujourd'hui pourraient, par suite des développements technologiques, devenir repersonnalisables demain.

À la protection de la vie privée conceptualisée uniquement sur le plan des renseignements identifiables se rattachait une deuxième préoccupation exprimée lors de la conférence. Il s'agit de la tendance nord-américaine qui consiste à considérer la protection de la vie privée uniquement comme un droit individuel contre l'intrusion de l'État, qu'on juxtaposait à l'approche européenne en vertu de laquelle la protection de la vie privée est un droit de la personne et un élément essentiel de la dignité humaine. Nos appréhensions quant aux répercussions sur la vie privée de bon nombre de technologies concernent la personne, mais aussi la société de façon générale. Ces préoccupations ont été exprimées de façon claire durant les séances sur l'informatique ubiquiste et le repérage géodépendant. En ce qui touche les répercussions de l'informatique ubiquiste, David Phillips a indiqué que nous devrions réfléchir aux questions entourant la diffusion, la collecte et la conservation de données dans le cadre des produits culturels diffusés sur le marché⁵⁹. Selon lui, les gens s'intéressent aux données non seulement parce qu'elles pourraient les identifier, mais aussi pour l'usage que l'on peut en faire en combinaison avec les données d'autres personnes, de manière à agir sur la culture dans laquelle elles vivent.

L'utilisation des données recueillies auprès de diverses personnes dans le but de créer des profils de groupe peut constituer un exemple probant de la façon dont les données servent de matériau de base pour produire et reproduire de la culture. David Lyon a expressément abordé la question des profils de groupe dans le contexte des données recueillies par

⁵⁸ L. Sweeney, note 49 ci-dessus.

⁵⁹ David Phillips aborde le concept de « développement des connaissances distribuées » dans ses observations à la première séance plénière de la conférence intitulée « L'informatique ubiquiste » (27 septembre 2007), voir diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_plenary1_02_f.ppt#369,11, L'internet des choses : ...alors pourquoi pas des personnes.

l'entremise des technologies du repérage géodépendant. Il a recensé les manières de regrouper les données sur des personnes afin de dresser des profils et de répartir les personnes en groupes sociaux. Il a prédit que ces types de tri auraient de vastes répercussions sociales, avec des conséquences particulièrement négatives pour les groupes déjà les plus marginalisés de la société⁶⁰. Ainsi, ce n'est pas seulement la personne dont on a recueilli au départ les données qui est touchée, mais également des membres d'autres groupes qui seront associés à un profil par l'intermédiaire du recoupement des données, les groupes eux-mêmes et la société en général.

Les participants de la conférence se sont entendus pour reconnaître qu'une politique sous-tendue par une conception selon laquelle la protection de la vie privée constitue un droit de la personne plutôt qu'un simple droit contre l'intrusion, à savoir l'accès aux renseignements qui rendent une personne identifiable, permettrait sans doute de mieux donner suite aux difficultés qui se posent à une époque où la diffusion, la collecte et la surveillance des données ne cessent de prendre de l'ampleur. Cette approche pourrait également offrir une plate-forme utile à partir de laquelle mieux mobiliser le public étant donné qu'elle ajoute à la protection de la vie privée une valeur sociale qui va au-delà de la protection contre l'identification individuelle. Bien qu'il subsiste d'excellentes raisons de s'inquiéter de l'utilisation des données pour identifier et suivre une personne, ce type d'approche pourrait à lui seul ne pas frapper l'imaginaire d'un segment important de la population qui croit n'avoir « rien à cacher ».

B. Protection de la vie privée et sécurité

Dans ce monde de l'après-11 septembre 2001, nous nous débattons constamment avec une proposition voulant que les sociétés démocratiques acceptent d'échanger la protection des renseignements personnels contre une sécurité accrue, comme si l'un et l'autre devaient inévitablement s'opposer. Sous l'influence de toute la publicité sur les risques posés à la sécurité physique du public, bon nombre de membres du grand public ne sont que trop pressés d'abandonner la protection de la vie privée pour améliorer la sécurité. La dichotomie entre la protection de la vie privée et la sécurité devient alors un outil rhétorique utile non seulement pour obtenir une multitude de concessions en matière de protection de la vie privée, mais aussi pour remettre en question les motifs et stratégies de ceux qui plaident en faveur de vigoureuses mesures de protection de la vie privée. Les participants de la conférence ont abordé la dichotomie d'au moins deux manières différentes.

Premièrement, ils ont récusé l'opposition « protection de la vie privée » et « sécurité » en la présentant comme une fausse dichotomie, bien que les motivations des uns pour remettre en question la dichotomie tranchaient nettement avec celles des autres.

⁶⁰ David Lyon exprime des inquiétudes quant à l'effet disparate du tri social sur les groupes marginalisés dans ses observations au premier atelier de la conférence intitulé « Le système de repérage géodépendant » (26 septembre 2007), voir diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop1_01_f.ppt#284,13, Slide 13.

Michael Chertoff, secrétaire du département de la Sécurité intérieure (DSI)⁶¹, s'appuyait sur l'analyse de la fausse dichotomie pour justifier les politiques de plus en plus envahissantes en matière de contrôle frontalier. Le secrétaire a indiqué que l'analyse préliminaire actuelle des passagers réduisait les intrusions dans la vie privée de la grande majorité du public en diminuant le nombre de passagers qui allaient faire l'objet d'un deuxième examen à la frontière. Ce type d'analyse pourrait bien séduire bon nombre de membres du public qui se voient eux-mêmes comme n'ayant « rien à cacher ». Toutefois, l'analyse omettait de prendre en compte les vastes répercussions sociales de l'accumulation et de la rétention des données non seulement aux fins d'avoir des rapports avec des gens, mais aussi pour trier des catégories entières de personnes et les associer à des profils.

Barry Steinhardt de l'ACLU⁶² a également remis en question la dichotomie entre la protection de la vie privée et la sécurité, mais pour des raisons tout à fait opposées à celle du secrétaire Chertoff. Selon Steinhardt, la dichotomie semble présumer une corrélation entre une moins grande protection de la vie privée et une plus grande sécurité. Comme il l'a habilement démontré, nous disposons toutefois de très peu de preuves selon lesquelles des concessions en grand nombre en matière de protection de la vie privée aient pu engendrer des gains sur le plan de la sécurité, et il ne se trouve aucun système en place permettant de contrôler ou de quantifier l'efficacité du prétendu compromis.

Bruce Schneier, qui a également mis en doute le concept selon lequel une moindre protection de la vie privée engendrait une plus grande sécurité, a offert aux participants une perspective légèrement différente sur cette dichotomie⁶³. Schneier était d'avis qu'elle était tout simplement erronée, et que la vraie question en jeu était celle qui opposait la liberté et le contrôle. Nous entrons dans une ère où les enregistrements des transactions sont accessibles pour pratiquement chaque interaction, et où ces enregistrements reposent entre les mains de tiers plutôt qu'entre celles des sujets sources, de sorte que les gens ont de moins en moins de prise sur leurs propres renseignements. Comme les membres du secteur commercial privé et le milieu de l'application de la loi reconnaissent la valeur que représente l'accès à ces entrepôts de données, la liberté individuelle se retrouve donc au beau milieu. Les approches de ce type ont amené plusieurs participants de la conférence à examiner la manière dont les développements technologiques nous font remettre en question la pertinence et la validité continue des approches juridiques en matière de protection des renseignements personnels dans bon nombre d'administrations.

C. Incohérences dans les approches juridiques existantes

Les participants de nombreux groupes d'experts de la conférence (circulation des données, forage de données, technologies fondées sur l'emplacement, mise en banque de

⁶¹ Discours liminaire prononcé lors de la conférence par Michael Chertoff, secrétaire, département de la Sécurité intérieure (26 septembre 2007).

⁶² Barry Steinhardt, première séance plénière de la conférence « Dragons : La sécurité publique et la mondialisation » (26 septembre 2007), voir diapositives en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_plenary1_01_f.ppt#269,3,Slide 3.

⁶³ Bruce Schneier, première séance plénière de la conférence « Dragons : La sécurité publique et la mondialisation » (26 septembre 2007).

substances biologiques) ont soulevé d'importantes préoccupations non seulement sur le caractère non adéquat des conceptions individualistes actuelles de la protection de la vie privée, mais aussi sur la manière dont on rend ces concepts opérationnels. Quatre d'entre eux retiendront ici notre attention : (i) les modèles fondés sur le consentement, le contrôle et la propriété; (ii) la structure des règles juridiques entourant les territoires physiques; (iii) les modèles axés sur la conservation et l'utilisation des données plutôt que sur la réduction; (iv) le modèle hiérarchique canadien des intérêts privés.

(i) Modèles fondés sur le consentement, le contrôle et la propriété
L'un des thèmes qui s'est clairement dégagé de la conférence était qu'un modèle juridique de protection de la vie privée selon lequel les données appartiennent aux personnes et qu'il faut les aider à garder prise sur ce qui leur appartient pourrait bien devenir obsolète et inefficace pour préserver les aspects fondamentaux de la dignité humaine et les visions sociales élargies d'une démocratie efficace, telle que les sous-tendent les protections de la vie privée. Les participants ont exprimé à cet égard des appréhensions à la fois pratiques et fondées sur des principes.

Du côté pratique, bon nombre de participants se sont interrogés sur la pertinence de l'avis de consentement à la collecte, à l'utilisation et à la conservation des données. Les membres du groupe d'experts qui se penchait sur les expériences en ligne des enfants ont exprimé de vives inquiétudes quant à savoir si l'on communiquait adéquatement aux enfants ou à leurs parents, dans un langage suffisamment simple pour qu'ils puissent les comprendre, les politiques sur la protection de la vie privée et les utilisations commerciales des données⁶⁴. Parallèlement aux préoccupations sur la pertinence de l'avis de consentement évoqué dans le premier cas, plusieurs conférenciers ont discuté des difficultés d'expliquer les utilisations secondaires de manière compréhensible pour les utilisateurs⁶⁵. En ce qui a trait à la génétique et à la mise en banque de substances biologiques, les intervenants ont exprimé des réserves sur la mesure dans laquelle les modèles binaires prennent en compte les données des sources de données uniquement à l'étape de la collecte, et sur les difficultés liées à l'élaboration de modèles conçus pour permettre d'obtenir à nouveau le consentement par rapport aux utilisations ultérieures proposées⁶⁶. Finalement, en ce qui touche la circulation des données entre gouvernements, les attentes en matière de protection de la vie privée de la part des utilisateurs qui « consentent » à ce qu'on recueille leurs données dans une juridiction pourraient bien être compromises par la circulation de ces données à des fins d'entreposage ou d'analyse dans une autre juridiction, dont les normes et les règlements en matière de protection de la vie privée peuvent être tout à fait différents⁶⁷. Par conséquent, même si l'on demeure engagé sur le plan conceptuel envers un modèle de gouvernance juridique fondé sur le consentement individuel, sa mise en œuvre est

⁶⁴ Premier atelier de la conférence « Sensibilisation à la protection de la vie privée des enfants », parties I et II (28 septembre 2007), conférenciers : Marita Moll, Thomas Hillman, Melissa Luhtanen et Cathy Wing, en ligne : http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop1_03_f.ppt#257,1,Slide 1.

⁶⁵ Voir la séance de la conférence sur « Le forage des données », note 11 ci-dessus.

⁶⁶ Voir la séance de la conférence sur « La génétique et la mise en banque de substances biologiques », note 21 ci-dessus.

⁶⁷ Voir la séance de la Conférence sur « La circulation et le miroitage de données », note 7 ci-dessus.

entravée par des problèmes très pratiques que risque d'exacerber le caractère de plus en plus présent de l'informatique.

Il a également été question de préoccupations fondées sur les principes, et qui concernent la pertinence conceptuelle du modèle axé sur le « consentement » individuel. Dans le contexte de l'informatique ubiquiste, les participants se demandaient s'il était souhaitable que soient relégués à une affaire de décision individuelle des aspects fondamentaux des relations sociales qui sont pertinentes pour la collectivité dans son ensemble⁶⁸. Prenons par exemple la question de la diffusion et de la réception omniprésentes des données. Une fois que les personnes ont accepté que leurs données soient continuellement accessibles à des fins de collecte, nous risquons de mettre en place une société dans laquelle la présomption de surveillance prévaudra étant donné qu'on ne disposera pas d'un choix individuel de refus. Dans le même ordre d'idées, d'importantes raisons nous poussent à remettre en question la légitimité des modèles axés sur le « consentement », qui reposent sur une conception des données basée sur la propriété. Bien que nous puissions nous satisfaire de l'idée que les personnes « possèdent » leurs propres données (quoique ces données soient de moins en moins en leur possession), nous devrions peut-être nous montrer moins optimistes lorsqu'il est question d'agrégation des données sur les collectivités dans leur ensemble. Sachant que, dans le contexte du repérage géodépendant ainsi que de la génétique et mise en banque de substances biologiques, les données individuelles servent parfois à dresser des profils et trier des collectivités de gens (à leur « avantage » dans certains cas), nous pourrions légitimement demander si une règle juridique fondée sur l'obtention du consentement des membres individuels de ces collectivités constitue un consentement adéquat en rapport avec les caractéristiques et le profil de la collectivité dans son ensemble. Pour résumer, à qui appartient la réputation et les caractéristiques de collectivités au complet?

(ii) Règle juridique fondée sur les territoires physiques

Les problèmes liés à la règle juridique fondée sur les territoires physiques ont nettement figuré parmi les thèmes de la conférence. La circulation des données basée sur les modèles d'affaires sans égard aux frontières pose de lourds obstacles aux régimes locaux dont la légitimité a toujours été définie par les frontières territoriales physiques. Par conséquent, il semblerait que les efforts intergouvernementaux et multisectoriels concertés abordés précédemment deviendront de plus en plus cruciaux pour l'élaboration et l'application des normes juridiques.

(iii) Efforts axés sur la conservation et l'utilisation plutôt que sur la réduction

L'importance de prendre des mesures proactives à l'égard des données représente un autre thème débattu lors de la conférence. Compte tenu de la facilité relative avec laquelle on peut analyser et contrôler les données recueillies, pour des fins de surveillance publique et privée, il semble logique de réorienter les règles juridiques sur la réduction de la collecte de données en tout premier lieu. Les démarches prises dans le sens de ce type de réglementation proactive se constatent facilement dans les pratiques de traitement équitable de l'information des lois canadiennes en matière de protection des

⁶⁸ Voir la séance de la conférence sur « L'informatique ubiquiste », note 23 ci-dessus.

renseignements personnels⁶⁹, dans le projet exploratoire de l'APEC⁷⁰, et dans les lois américaines visant à limiter les données recueillies par les organismes de services sociaux et les refuges pour les femmes qui fuient un climat de violence familiale⁷¹. Les initiatives de réduction des données pourraient jouer un rôle important pour les établissements de vente au détail et les institutions financières, car leur stockage de grandes quantités de données en fait des cibles de premier choix pour le piratage en ligne, les logiciels malveillants et la fraude⁷².

(iv) Caractère inadéquat du modèle hiérarchique canadien

Le système juridique canadien est peut-être aux prises avec des défis uniques en ce qui touche la protection des renseignements personnels, du moins pour ce qui est de son approche actuelle consistant à imposer des limites constitutionnelles aux pouvoirs de l'État en matière de recherche et de saisie. Comme l'a rappelé Ian Kerr aux participants de la conférence, les tribunaux canadiens ont rendu une quantité considérable de décisions sur la protection de la vie privée par suite de contestations des recherches et saisies effectuées par l'État⁷³. Dans le cadre de cette jurisprudence, on a théoriquement catégorisé par ordre d'importance décroissante les intérêts liés la vie privée, allant des questions d'ordre physique à celles liées à l'emplacement, puis à l'information⁷⁴. Dans un monde d'informatique ubiquiste où les gens fournissent des données sur eux-mêmes et l'endroit où ils se trouvent, ces catégories deviennent de plus en plus floues. Une situation où les plaintes portant sur des « données » entrent uniquement dans la catégorie « information » pourrait bien compromettre la protection juridique de la vie privée au Canada. Les décisions juridiques qui ont trait aux préoccupations liées à la protection de la vie privée et sont formulées hors du contexte des limites imposées à la recherche et à la saisie, comme dans le cas de la récente décision de la Cour supérieure de justice de l'Ontario sur la divulgation des renseignements relatifs à l'adoption⁷⁵, offrent d'excellentes occasions d'élaborer une conception de la vie privée où l'on prend mieux en compte les droits de la personne plutôt qu'une conception dont l'orientation centrale est celle des libertés individuelles.

⁶⁹ Commissariat à la protection de la vie privée du Canada, « Guide à l'intention des entreprises et des organisations : Protection des renseignements personnels : vos responsabilités : La Loi sur la protection des renseignements personnels et les documents électroniques du Canada » (26 avril 2004), en ligne : http://www.privcom.gc.ca/information/guide_f.asp#009.

⁷⁰ APEC Privacy Pathfinder, note 35 ci-dessus.

⁷¹ *Violence Against Women Act*, note 32 ci-dessus.

⁷² Voir l'exposé présenté à la conférence par Dean Turner sur « Le crime sur Internet », note 30 ci-dessus.

⁷³ Ian Kerr exprime des inquiétudes quant à l'approche juridique canadienne en matière de protection de la vie privée dans ses observations à la première séance plénière de la conférence intitulée « L'informatique ubiquiste » (27 septembre 2007), note 23 ci-dessus.

⁷⁴ *R c. Tessling*, [2004] 3 R.C.S. 432.

⁷⁵ *Cheskes c. Ontario*, [2007] O.J. No. 3515 (SCJ).

CONCLUSION

Conscients du fait que l'horloge continue d'avancer pendant que nous prenons une pause pour réfléchir à l'ampleur et à la profondeur des défis que les nouvelles technologies posent à la protection de la vie privée et, par conséquent, à la dignité humaine et à l'équité, il serait bon d'examiner sous un éclairage différent le symbole du dragon évoqué lors de la conférence *Terra Incognita*. Le dragon de la conférence évoque l'animal médiéval tel que représenté dans le folklore européen et nord-américain, à savoir une créature maléfique et menaçante qu'il vaut mieux tuer pour protéger les masses innocentes. Dans les cultures asiatiques anciennes, on trouve un dragon très différent, un symbole de pouvoir aux formes changeantes qui mérite vénération. Les gens nés au cours de l'année du dragon possèdent un pouvoir inné⁷⁶. Pour ceux qui se soucient de protéger la vie privée et les valeurs qui les sous-tendent, ce dragon peut servir de guide.

Bien qu'il soit clair que nous devons nous attaquer aux menaces externes posées à la protection de la vie privée et prenant diverses formes dans un contexte de mondialisation, de technologies nouvelles et de crimes sur Internet, les dragons inhérents à ces menaces présentent peut-être l'obstacle le plus difficile à résoudre. La façon dont le milieu de la protection de la vie privée mobilise le cœur et l'esprit des membres de la grande collectivité qui croient n'avoir rien à cacher et démontrent un appétit apparemment insatiable en matière d'information sur les autres pourrait se révéler aussi cruciale dans la bataille que toute autre initiative et technique élaborée pour contrôler les pratiques de gestion des données.

Alors que nous nous efforçons de moderniser nos instruments réglementaires et de repenser les concepts juridiques fondamentaux qu'on estimait autrefois aptes à protéger la vie privée, il est à souhaiter que l'attention accordée à la *terra incognita* ne nous empêchera pas de s'occuper des dragons qui, nous le savons, se trouvent parmi nous ainsi qu'en nous tous.

⁷⁶ Pour de plus amples échanges sur ces questions, voir C.A.S. Williams, *Chinese Symbolism & Art Motifs* (Tuttle Publishing, 1941) p. 132.

ANNEXE A

Résolution sur l'urgence d'établir des normes mondiales visant la protection des données des passagers dont se serviront les gouvernements pour appliquer les lois et assurer la sécurité frontalière

**29^e Conférence internationale des commissaires à la protection des données et de la vie privée
Montréal, Canada,
25-28 septembre 2007**

Auteur de la proposition : Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (Allemagne)

Co-parrains :

Österreichische Datenschutzkommission (Autriche)
Commissariat à la protection de la vie privée du Canada (Canada)
Office of the Information and Privacy Commissioner of British Columbia
[Colombie-Britannique]
Office of the Information and Privacy Commissioner of Ontario
European Data Protection Supervisor (Union européenne)
La Commission Nationale de l'Informatique et des Libertés (France)
Landesbeauftragte für Datenschutz und die Informationsfreiheit Nordrhein-Westfalen (Allemagne – régional)
Garante per la protezione dei dati personali (Italie)
College Bescherming Persoonsgegevens (Pays-Bas)
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Roumanie)
Agencia de Protección de Datos (Espagne)
Préposé fédéral à la protection des données (Suisse)
Information Commissioner (R.-U.)

La Conférence rappelle :

- que le communiqué adopté lors de sa 24^e réunion à Cardiff en 2002;
- que la résolution sur le transfert des données des passagers, adoptée lors de sa 25^e réunion internationale à Sydney en 2003;
- que la déclaration sur la protection des données personnelles et de la vie privée dans un cadre de mondialisation, adoptée lors de sa 27^e réunion internationale à Montreux à 2005;

ont pour objet de reconnaître l'équilibre à établir entre la lutte légitime contre le terrorisme et la criminalité internationale, et les droits des personnes à la protection des données et de la vie privée.

La Conférence retient :

- que les gouvernements cherchent de plus en plus en plus à obtenir des renseignements sur les passagers pour s'en servir dans la lutte contre le terrorisme, l'immigration illégale et d'autres crimes sans accorder toute la considération voulue à la protection de la vie privée et des droits des passagers;
- que certains renseignements sur les passagers peuvent servir à tirer des conclusions sur la religion, l'ethnicité et d'autres questions très délicates;
- que bon nombre de gouvernements autour du monde réclament de plus en plus de données des transporteurs;
- que les transporteurs recueillent des données sur les passagers à des fins commerciales, et qu'on leur demande de les fournir à des fins d'application de la loi;
- que les transporteurs sont de plus en plus appelés à répondre à de nombreuses et diverses demandes de données et à se conformer à de nombreux et divers systèmes de transfert des données, ce qui crée de l'incertitude parmi eux et les passagers quant à leurs droits et obligations, et fait en sorte qu'il est difficile pour les passagers de comprendre l'utilisation faite de leurs données, en plus du risque de voir les transporteurs transférer les données de manière inappropriée;
- que ces demandes et systèmes nombreux et variés impliquent des coûts pour les lignes aériennes et les passagers;
- qu'il faut faire preuve de cohérence technique et juridique pour s'assurer que les transporteurs répondent à ces demandes;
- que certains transporteurs ne se conforment pas encore tout à fait à leurs obligations d'informer les passagers sur l'utilisation et la communication de leurs données;
- que d'autres arrangements mondiaux ont été mis en place pour faciliter les voyages aériens, et qu'il est urgent d'élaborer des solutions à cette échelle tout en respectant les droits des passagers à la protection de leur vie privée.

La Conférence réaffirme :

- que le droit à la protection des données et de la vie privée, tel que garanti dans l'article 12 de la Déclaration universelle des droits de l'homme et par d'autres instruments juridiques, protège les personnes et leurs renseignements personnels, et qu'il faut le prendre en considération en même temps que d'autres droits dans toute proposition impliquant le transfert et l'utilisation des renseignements sur les passagers à des fins d'application de la loi;
- que le traitement des renseignements sur les passagers devrait se dérouler dans un cadre qui tient compte des normes et des principes acceptés en matière de protection des données;

- que le gouvernement devrait démontrer que toute proposition de sa part visant à faire usage des renseignements sur les passagers :
 - est nécessaire pour répondre à un problème particulier;
 - résoudra vraisemblablement le problème;
 - est proportionnelle aux avantages sur le plan de la sécurité;
 - implique une moindre intrusion dans la vie privée que ne le feraient d'autres options;
 et qu'il faudrait la réviser régulièrement pour s'assurer que les mesures dont elle est assortie restent proportionnées;
- que la nécessité de protéger la vie privée dans toute situation qui se présente demeure une tâche essentielle non seulement pour la communauté mondiale de la protection des données personnelles, mais aussi pour tous ceux qui sont concernés par les droits et libertés fondamentaux;
- que si les gouvernements n'appliquent pas une approche permettant de pondérer correctement les préoccupations liées à la protection des données et de la vie privée, nous risquons d'assister à un glissement dangereux susceptible de saper les libertés les plus fondamentales qu'ils cherchent à protéger.

Dans la poursuite de normes mondiales de protection des données et, par conséquent, de la préservation des renseignements sur les passagers dont se serviront les gouvernements à des fins d'application de la loi et de sécurité frontalière, la Conférence demande :

- que les organisations internationales (telles que l'Association du transport aérien international [IATA] et l'Organisation de l'aviation civile internationale [OACI]), les gouvernements et les transporteurs joignent leurs efforts à ceux des commissaires à la protection des données et de la vie privée pour adopter des solutions mondiales ayant force exécutoire et assorties de mesures appropriées pour la protection des données;
- que le gouvernement démontre que toute proposition de sa part visant à faire usage des renseignements sur les passagers :
 - est nécessaire pour répondre à un problème particulier;
 - résoudra vraisemblablement le problème;
 - est proportionnelle aux avantages sur le plan de la sécurité;
 - implique une moindre intrusion dans la vie privée que ne le feraient d'autres options;
 et qu'on la réviser régulièrement pour s'assurer que les mesures dont elle est assortie restent proportionnées;
- que tout programme gouvernemental pour lequel il est fait usage de renseignements sur les passagers comporte des procédures visant : une utilisation minimale de tels renseignements; l'établissement de limites explicites pertinentes aux fins du programme quant à l'utilisation, la communication et la conservation de tels renseignements; l'assurance de la précision des données; les droits d'accès et les corrections nécessaires; enfin, la réalisation d'un examen indépendant;

- que toute solution soit appliquée en tenant compte des enjeux juridiques, techniques et financiers des transporteurs et des autorités ainsi que dans le souci de l'efficacité de leur travail;
- que les gouvernements soient ouverts et transparents quant aux raisons pour lesquelles les données sont recueillies et utilisées, et qu'ils s'assurent que tous les passagers, peu importe leur citoyenneté ou leur pays d'origine, puissent accéder à leurs renseignements personnels et recourir à des mécanismes de recours adéquats;
- que les transporteurs renseignent adéquatement leurs passagers sur l'utilisation et la communication de leurs données au gouvernement et aux organismes d'application de la loi, sur toute utilisation de listes de personnes interdites de vol ou autres listes de surveillance, ainsi que sur les mesures de recours existantes en ce qui touche l'utilisation et la précision des renseignements sur les passagers et des renseignements personnels connexes;
- que les commissaires à la protection des données et de la vie privée continuent à travailler ensemble afin d'assurer la mise en place de mesures appropriées pour la protection des données et de la vie privée, et qu'ils fassent pression en faveur de l'application de solutions mondiales ayant force exécutoire.

Note explicative

Les gouvernements de différents pays cherchent de plus en plus à utiliser les renseignements sur les passagers comme outil pour contrer le terrorisme, la criminalité transnationale et autres formes d'activités criminelles. Cette façon de faire a engendré des différences dans les éléments d'information demandés, l'utilisation qui en est faite et le niveau de mesures de protection mises en place.

Le caractère des voyages internationaux est tel qu'il faut recourir à une approche globale et trouver de toute urgence une solution mondiale pour assurer des niveaux pertinents de sécurité et inspirer confiance aux passagers, tout en offrant des mesures proportionnées qui incluent les protections nécessaires pour les données et la vie privée.

Bien qu'il soit primordial, dans la recherche d'une solution mondiale, de donner suite aux préoccupations entourant la protection des données et de la vie privée, il faut également que cette solution permette de tenir compte d'autres préoccupations des lignes aériennes et des passagers qui sont de caractère juridique, technique et financier et qui concernent également l'efficacité.

Des normes mondiales peuvent apporter l'équité, la cohérence, la conformité juridique et des protections pour les passagers comme pour les lignes aériennes. Il va de soi que les transporteurs, les organismes d'application de la loi, les organisations internationales, les groupes de la société civile et les experts en protection des données et de la vie privée doivent tous contribuer à la quête d'une solution mondiale. Il est également essentiel, si l'on veut faire des progrès, que les commissaires à la protection des données et de la vie privée s'engagent à diriger les efforts dans la pression exercée pour dégager une telle solution.

ANNEXE B

Déclaration des organisations de la société civile sur le rôle des commissaires à la protection des données et de la vie privée

Montréal, le 25 septembre 2007

Nous représentons des organisations de la société civile qui se sont réunies à Montréal en septembre 2007, à la veille de la Conférence internationale des commissaires à la protection des données et de la vie privée, et nous avons fait consensus sur plusieurs points importants que nous aimerions soumettre aux commissaires à la protection de la vie privée du monde entier. Ensemble nous déclarons que :

1. Nous voyons nos sociétés renoncer, à un rythme alarmant, à des valeurs et à des droits fondamentaux touchant la protection de la vie privée et de l'autonomie personnelle.
2. Nous assistons à la mise en place d'une infrastructure sans précédent pour la surveillance des personnes et des groupes à l'échelle mondiale. Cela comprend la mise au point de systèmes, inimaginables encore récemment, visant à surveiller nos déplacements : repérage des voyageurs, profilage des passagers au moyen de puissants logiciels de cueillette de données — banques de données de dossiers passagers (DP), systèmes avancés de renseignement sur les passagers (APIS), systèmes de contrôle des entrées et sorties — et de nouveaux systèmes pour retracer l'identité des personnes. Nous remarquons un recours croissant aux ressources de la technologie — étiquettes d'identification par radiofréquence, biométrie, ADN, forage des données, télévision en circuit fermé, et plusieurs autres — afin de suivre nos allées et venues à l'intérieur des pays, des collectivités et même des écoles. Nous découvrons sans cesse l'existence de nouvelles méthodes d'écoute de nos communications. Tous ces systèmes, et d'autres encore, entraînent une prolifération de bases de données de renseignements personnels et l'application de nouveaux outils pour explorer, combiner et évaluer rapidement le contenu de ces banques informatiques.
3. Ces systèmes de surveillance sont érigés tant par les États que par le secteur privé. On ne peut que s'inquiéter de la convergence croissante entre les activités de surveillance de l'État et celles de l'entreprise privée.
4. Ces systèmes sont souvent développés sans débat démocratique, sans autorisation et sans contrôle. Par conséquent, les avantages qu'on leur prête sont trop souvent acceptés sur parole, sans qu'on ait pris le temps de bien examiner si leur intrusion dans notre vie privée se limite à ce qui est nécessaire et raisonnable.
5. Les systèmes juridiques de nos pays ont largement échoué à suivre l'essor des nouvelles technologies invasives. Même lorsqu'on cherche à obtenir l'autorisation des élus, ceux-ci sont loin de toujours disposer d'une information adéquate sur ces nouveaux produits. Dans certains de nos pays, les institutions judiciaires cèdent trop souvent aux demandes du pouvoir exécutif alors qu'ailleurs on n'instruit que rarement des causes sur ces enjeux parce que les organisations de la société civile n'ont pas les moyens d'avoir recours aux tribunaux.

6. Nous sommes témoins d'une érosion des droits individuels qui dépasse encore la somme de tous ces développements – une société où la surveillance se fait de plus en plus omniprésente.
7. Même si nos pays se rappellent tous avoir affronté des menaces et des crises plus graves que le terrorisme, les hauts responsables de la sécurité ont su exploiter la crainte du terrorisme et de la criminalité internationale pour accroître leur pouvoir et battre en brèche la protection juridique de la vie privée, et ils collaborent de plus en plus au niveau transnational pour appuyer leurs objectifs respectifs.
8. Les commissaires à la protection de la vie privée occupent une position privilégiée pour résister à cet assaut contre le droit à la vie privée et les valeurs fondamentales de nos sociétés.

C'EST POURQUOI nous estimons que les commissaires à la protection de la vie privée doivent prendre des mesures plus vigoureuses, plus agressives, pour s'attaquer au problème. Il est énorme. Pour l'endiguer, les rapports ponctuels, les mises en garde et les mesures coercitives, quoique souvent utiles, ne suffiront pas. Plus précisément :

- Les commissaires à la protection de la vie privée doivent étendre leur mission, accorder plus d'attention à l'ensemble du phénomène de l'érosion de la vie privée et contester plus vigoureusement l'orientation que prennent nos pays. Trop de commissions de protection de la vie privée sont devenues de simples agences administratives, ou se laissent intimider par l'agressivité des services de sécurité qui invoquent la menace du terrorisme pour justifier différentes atteintes à la vie privée.
- Nous en sommes convaincus, le problème est urgent : l'accélération de l'innovation technologique et l'accroissement du potentiel de surveillance qu'elle offre à l'État et au secteur privé nous obligent à agir rapidement pour éviter de nous retrouver devant le fait accompli d'une société de surveillance totale.
- Les commissaires à la protection de la vie privée se doivent d'accroître leurs efforts collectifs pour protéger la vie privée contre l'accroissement de la collaboration transfrontalière mise en oeuvre par l'establishment mondial de la sécurité.
- Il faut que les commissaires à la protection de la vie privée interviennent avec force auprès de leurs gouvernements respectifs pour les inciter à résister aux pressions, visant à affaiblir les normes existantes de protection de la vie privée, exercées par les États-Unis, d'autres pays ou des instances régionales. Au sein de la communauté mondiale, les pratiques répréhensibles d'un seul pays peuvent miner les systèmes de protection de la vie privée de tous.
- Dans ce contexte, les commissaires à la protection de la vie privée devraient intervenir activement auprès du public et des médias, et faire appel aux tribunaux, s'il y a lieu. Les commissaires devraient exiger que les initiatives gouvernementales affectant la vie privée fassent l'objet de débats publics et de décisions démocratiques. Les commissaires devraient lutter activement pour la création de mécanismes de contrôle capables d'assurer au public une protection permanente contre les programmes intrusifs.
- Les commissaires à la protection de la vie privée devraient anticiper l'impact des services commerciaux sur la vie privée et intervenir avant que de tels services ne

- soient implantés de manière irrémédiable. Et ils devraient coordonner leurs efforts à l'échelle de ce qui devient de plus en plus un marché mondial.
- Il faut un effort concerté au niveau transnational pour préserver les droits humains fondamentaux et s'assurer que les individus ne soient pas surveillés de manière routinière dans leurs mouvements et leurs activités quotidiennes : ces libertés sont essentielles en démocratie.
 - À nos gouvernements, nous demandons aussi d'accroître l'autorité et l'indépendance des commissaires à la protection de la vie privée pour renforcer les institutions vouées à la protection des données et de la vie privée, ou de créer ces institutions là où elles n'existent pas.

Signataires :

- American Civil Liberties Union (ACLU)
- Association pour les libertés civiles de Colombie-Britannique (BCCLA)
- Australian Privacy Foundation (APF)
- BC Freedom of Information and Privacy Association (FIPA)
- Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC)
- Coalition pour la surveillance internationale des libertés civiles (CSILC) qui représente 38 organisations de la société civile au Canada
- Electronic Privacy Information Center (EPIC)
- European Digital Rights (EDRi)
- Imaginons un réseau Internet solidaire (IRIS), France
- Ligue des droits et libertés (Québec)
- North American Consumer Project on Electronic Commerce (NACPEC), Mexique
- Option Consommateurs (Quebec)
- Privacy International
- Statewatch