

**Instaurer la confiance :
sécurité, protection de la vie privée et
autonomisation des utilisateurs**

*Un document de discussion préparé pour la
Table ronde du Canada sur l'avenir de l'économie Internet
Ottawa, 2 octobre 2007*

Michael Geist
Chaire de recherche du Canada en droit d'Internet et du commerce électronique
Université d'Ottawa, Faculté de droit

Les opinions exprimées dans ce document sont celles de l'auteur et ne représentent pas
nécessairement celles d'Industrie Canada ou du Gouvernement du Canada.

L'année dernière, le choix de la revue Time pour la personnalité de l'année s'est arrêté sur « Vous » (une référence aux personnes derrière le contenu généré par les utilisateurs sur Internet). Tourné en dérision par les critiques, ce choix a été jugé mauvais car il négligeait le travail de plusieurs dirigeants politiques notables. Pourtant, il y a lieu de considérer ce choix comme un point tournant : l'intégration de l'Internet participatif en plein essor – qui comprend des millions de blogueurs, de mixeurs de musique, de créateurs de vidéos amateurs, de journalistes citoyens, de wikipédiens et de photographe Flickr – dans le courant général.

Ce choix pourrait aussi amener les dirigeants gouvernementaux et les responsables de l'élaboration de politiques à réfléchir à leur place dans le monde de l'Internet participatif et des possibilités commerciales en ligne. Comme réaction initiale, ils pourraient fort bien rester à l'écart, à mesure que la vitesse de développement et l'énorme énergie créative semblent être en désaccord avec la lenteur prodigieuse des processus gouvernementaux d'élaboration de politiques. Bien qu'une réponse réglementaire solide soit certes inutile, voire nuisible, ce serait une erreur que de faire fi complètement de la question. Dans le milieu des années 1990, l'émergence de l'Internet et du commerce électronique ont suscité une approche engagée de la part du gouvernement, qui a trouvé un juste milieu entre le besoin d'un modèle d'auto-réglementation dirigé par le secteur privé et les lois sur le commerce électronique et la protection de la vie privée qui ont bâti la confiance des consommateurs et des entreprises à l'égard du nouveau mode de communication.

Le Canada : un participant à l'élaboration de politiques mondiales

Longtemps considéré comme un important participant à l'élaboration de politiques mondiales, le Canada a souvent servi de pont entre les points de vue divergents de l'Amérique du Nord, de l'Europe et de l'Asie. Bâter la confiance à l'égard de l'environnement en ligne pose, sans aucun doute, un défi mondial – peu importe la source, les préoccupations associées à la protection de la vie privée, à la sécurité et à la cybercriminalité touchent les consommateurs et les entreprises partout au monde. En effet, d'après un sondage mené en 2002 auprès d'internautes chinois, 94 % étaient préoccupés de la protection de leur vie privée et 65 % s'inquiétaient de la sécurité en ligne de leurs renseignements financiers. Ces résultats s'apparentent à ceux du Canada.

Pour relever ces défis, il faudra une **participation active à la gamme de tribunes mondiales**, y compris l'OCDE, le Conseil de l'Europe, l'APEC, l'OEA et l'UIT. De plus, les questions d'application transfrontalière de la loi devraient occuper une place dominante dans la stratégie internationale du Canada. Parmi ces questions, mentionnons l'élaboration de mécanismes internationaux efficaces qui faciliteraient une collaboration pour l'application transfrontalière de lois sur la protection de la vie privée, en plus de fournir une aide mutuelle dans l'application de ces lois, notamment par la notification, le

renvoi de plaintes, l'aide à l'enquête et le partage de l'information, sous réserve de mesures de protection appropriées.

En plus de sa contribution sur la scène mondiale, le programme national du Canada présente le potentiel de jouer un **rôle modèle pour d'autres pays** qui sont aux prises avec ces questions. La loi nationale du Canada sur la protection des renseignements personnels est souvent citée comme un modèle pour la loi de l'Union européenne sur la protection des données personnelles qui est en faveur des entreprises. Dans le même ordre d'idées, grâce à ses recommandations, le Groupe de travail national sur le pourriel a joué un rôle intégral dans l'élaboration d'une trousse d'outils internationale pour combattre le pourriel et les Principes d'authentification électronique ont servi de référence principale pour le récent document de recommandation et d'encadrement sur l'authentification du Conseil de l'OCDE. Ces expériences illustrent que les avantages de politiques saines et proactives élaborées au pays s'étendent bien au-delà de la scène nationale, car elles ont le potentiel de servir de base pour des lois et des politiques similaires dans le monde entier.

Le contexte canadien

Bon nombre de ces politiques – aussi bien nationales qu'internationales – ont profité aux Canadiens. L'Enquête canadienne sur l'utilisation d'Internet, menée par Statistique Canada en 2005, démontre qu'un pourcentage important de Canadiens utilisent maintenant régulièrement Internet pour une gamme de plus en plus variée d'activités. L'enquête a révélé que presque 17 millions de Canadiens – soit 68 % de la population adulte – utilisent Internet à des raisons personnelles non commerciales. De plus, près des deux tiers des adultes canadiens ont utilisé Internet à partir de leur domicile, tous les jours. Cela représente un virage social remarquable, car cela signifie que dix millions de Canadiens consacrent une partie de leur temps de loisir à domicile à Internet.

Lorsqu'ils sont en ligne, plus de la moitié des internautes canadiens utilisent le réseau pour le courriel (l'activité la plus répandue : 92 % des Canadiens ont indiqué utiliser le courriel), la navigation sur le Web, la visualisation des nouvelles et des sports, les transactions bancaires électroniques et le paiement de factures, ainsi que l'accès à l'information sur la météo, les voyages, la santé et les services gouvernementaux. Par ailleurs, plus de 40 % des internautes ont indiqué qu'ils s'étaient engagés dans le commerce électronique, l'éducation et les événements communautaires. Au cours des dernières années, nous avons également assisté à un groupe notable d'entreprises canadiennes qui ont servi de modèles de réussite. Des chefs de file comme Flickr, StumbleUpon, Club Penguin and Webkinz ont tous fait leurs débuts au Canada; et il existe des douzaines de nouvelles entreprises en gestation.

Malgré cette décennie impressionnante de réalisations, il n'en demeure pas moins que nous sommes toujours aux premières étapes d'un développement qui se dirige vers un accès universel, un déploiement plus rapide de la large bande, une plus grande puissance

informatique et un éventail plus large de contenu pour un réseau plus vivant, ainsi que de nouvelles possibilités commerciales, sociales et pédagogiques.

Bâtir la confiance : un programme général

Pour réaliser ce potentiel, un élément essentiel consiste à bâtir la confiance des entreprises et des consommateurs à l'égard du contexte en ligne. Vers la fin des années 1990, le « programme de la confiance » mettait l'accent sur des questions telles que la certitude du commerce électronique, la protection des renseignements personnels et la protection des consommateurs. De nos jours, la confiance est toujours un thème pertinent. En effet, d'après les données de Statistique Canada, les Canadiens craignent toujours les risques que pose Internet pour la sécurité et la protection des renseignements personnels : les trois quarts des répondants ont indiqué qu'ils étaient inquiets ou très inquiets de la sécurité et de la protection des renseignements personnels. Ces préoccupations englobent vraisemblablement les atteintes à la sécurité, l'abus des données personnelles ainsi que la prolifération du pourriel et des logiciels espions. Même si 57 % des internautes avaient fait du « lèche-vitrine en ligne » en 2005, seulement 43 % d'entre eux ont réellement commandé des produits ou services personnels. Cela laisse entendre que de nombreux Canadiens utilisent Internet pour faire des recherches sur des achats potentiels, mais demeurent réticents à l'idée de fournir des données sur leur carte de crédit ou d'autres renseignements personnels pour compléter la transaction.

À bien des égards, les préoccupations relatives à la confiance des consommateurs et des entreprises dépassent de loin les frontières étroites de la protection de la vie privée et de la sécurité. D'autres questions primordiales entrent en ligne de compte, notamment :

- la neutralité du réseau et les préoccupations des consommateurs à l'égard du manque de transparence et de concurrence sur le marché des services à large bande. Malgré les promesses de vitesses plus rapides et de fonctions plus puissantes de partage de fichiers, de nombreux consommateurs craignent de plus en plus que certains services offrent beaucoup moins que ce qui est annoncé dans leur publicité, car certains FSI s'adonnent activement au « remodelage du trafic », un processus qui limite la quantité de largeur de bande disponible pour certaines applications;
- les préoccupations relatives à l'établissement de prix et à la concurrence pour les données mobiles diminuent la confiance des consommateurs à l'égard des applications mobiles et la confiance des développeurs à fournir de tels produits et services au marché canadien. Comme les sociétés de télécommunications canadiennes traitent l'utilisation d'Internet mobile comme un produit d'affaires, elles ont établi des forfaits qui obligent la plupart des consommateurs à conserver leur temps en ligne de façon frugale;

Instaurer la confiance :
sécurité, protection de la vie privée et
habilitation des utilisateurs

- l'utilisation de la gestion des droits numériques (GDN) et le manque d'interopérabilité avec le contenu acheté en ligne. Par exemple, la controverse concernant le Sony Rootkit, dans laquelle la deuxième plus grande marque d'album du monde a rendu des centaines de milliers d'ordinateurs personnels vulnérables aux attaques de pirates informatiques car la société avait inséré un logiciel de protection de copie défectueux dans des douzaines de CD, ce qui a diminué la confiance des consommateurs à l'égard du marché de la musique;
- des règles de droit d'auteur restrictives qui ne distinguent pas la flexibilité du piratage. L'absence d'une disposition d'utilisation équitable au Canada a suscité l'appui des intervenants dans le milieu des droits d'auteur pour accroître la confiance à l'égard du cadre législatif du droit d'auteur au Canada. De nombreux groupes craignent que la loi actuelle entrave l'innovation, ce qui place le Canada dans une position désavantageuse par rapport à ses concurrents américains;
- les préoccupations liées à la liberté d'expression en ce qui concerne les diffamations en ligne, car de nombreux Canadiens n'ont pas assez confiance pour publier des commentaires en ligne, par crainte d'être poursuivis. Dans la foulée des récentes poursuites en justice, il se peut que de nombreux sites abandonnent tout simplement la capacité de publier des commentaires, car il sera trop onéreux de surveiller et de vérifier chaque commentaire. Comme solution de rechange, de nombreux sites pourraient laisser tomber leur présence en ligne au Canada et opter pour une présence en ligne aux États-Unis.

En raison de l'importance de ces questions, il peut être tentant de détourner l'attention des préoccupations en matière de sécurité et de protection des renseignements personnels dans le cadre des politiques. Or, ce serait une erreur puisque ces deux préoccupations constituent toujours des questions cruciales qui nécessitent encore beaucoup de travaux. Durant l'été 2007, les médias canadiens ont régulièrement relaté des incidents liés à la sécurité et à la protection des renseignements personnels sur Internet, notamment :

- une faille à la sécurité dans le site Monster.com, un site de recherche d'emploi de premier plan, qui a entraîné le vol de renseignements personnels de plus 1,3 millions de personnes;
- des menaces physiques à l'endroit d'Ujjal Dosanjh, un député, sur Facebook, le site de réseautage social chef de file du Canada;
- des préoccupations en matière de protection de la vie privée relativement à l'inclusion de vidéos personnels sur YouTube, sans permission;

- la croissance continue du pourriel, y compris l'utilisation de fichiers PDF et de pourriels basés sur des images afin de contourner les filtres anti-pourriel. En fait, une montée de pourriels qui imitaient le marché des cartes de souhait en ligne a menacé de détruire cette industrie autrement fructueuse;
- des avertissements répétés envoyés à des millions de Canadiens de la part des grandes banques, y compris la Banque Royale du Canada et la Banque Toronto-Dominion, au sujet des dangers de répondre aux courriels d'hameçonnage qui proviennent de sources légitimes;
- une attaque massive de déni de service en Estonie, un des pays les plus avancés sur le plan électronique au monde, ce que certains analystes considèrent comme le premier cas de « cyberguerre».

Ces incidents soulignent le fait que le cadre actuel de sécurité et de protection des renseignements personnels risque de ne pas être en mesure de faire face aux problèmes posés par la prochaine génération d'Internet. Les données de Statistique Canada montrent que les Canadiens s'adonnent à des activités Internet de « plus grande valeur » -- le gouvernement en direct, le commerce électronique et une participation plus active -- car ils acquièrent plus d'expérience et se sentent plus à l'aise dans l'environnement en ligne. En d'autres termes, il existe une corrélation directe entre la confiance à l'égard d'Internet et la volonté d'utiliser le réseau pour un éventail plus large d'activités. À mesure que des millions de Canadiens passent par cette courbe d'apprentissage, le gouvernement doit travailler avec des groupes du secteur privé et des partenaires internationaux afin d'élaborer un cadre juridique et stratégique, à l'échelle nationale et mondiale, qui renforce la confiance à l'égard du contexte en ligne.

Protection des renseignements personnels : permettre aux Canadiens d'avoir la mainmise sur leurs renseignements personnels

De façon générale, la loi canadienne sur la protection des renseignements personnels est conforme aux normes internationales. Toutefois, les Canadiens ont toujours des réserves quant à la protection de leurs renseignements personnels. Le vol de l'identité est devenu une activité criminelle importante; les transferts transfrontaliers de renseignements personnels ont suscité des débats animés dans la Chambre des communes; même la commissaire fédérale à la protection de la vie privée s'est retrouvée victime d'« usurpateurs », qui utilisent des techniques d'imitation pour saisir des renseignements personnels.

Pour régler ces problèmes, il faudra plus qu'une réforme nationale. Toutefois, la loi fédérale sur la protection des renseignements personnels constitue un bon point de départ. Une réforme évidente consiste à créer une exigence de **divulcation obligatoire des**

incidents d'atteinte à la sécurité, à l'instar des douzaines d'états aux États-Unis qui ont mandaté la divulgation d'incidents d'atteinte à la sécurité aux individus dont les renseignements personnels ont été mis à risque. Grâce à une loi sur la notification des cas d'atteinte à la sécurité, les individus reçoivent un avis pour atténuer les dommages potentiels d'un vol d'identité. Parallèlement, la loi crée des incitatifs pour une conformité organisationnelle en matière de sécurité et de protection des renseignements personnels.

Le Canada doit également commencer à régler la préoccupation croissante liée à l'impartition de renseignements personnels vers des organisations étrangères, particulièrement la **circulation transfrontalière des données** vers les États-Unis. Une telle impartition a pour conséquence d'assujettir potentiellement les renseignements personnels des Canadiens à la divulgation secrète en vertu des lois américaines, y compris la USA Patriot Act. Plusieurs provinces, dont la Colombie-Britannique, le Québec et la Nouvelle-Écosse, ont pris des mesures pour réduire la capacité des autorités américaines d'imposer la divulgation secrète. Le gouvernement fédéral n'a pas encore adopté des protections statutaires de la même nature, ce qui alimente les craintes selon lesquelles la loi canadienne sur la protection des renseignements personnels risque de devenir insignifiante face aux pouvoirs américains d'application des lois.

Les responsables canadiens de l'élaboration de politiques doivent également commencer à examiner notre cadre juridique actuel pour déterminer s'il peut **aborder adéquatement les technologies émergentes** qui risquent de ne pas être adaptées au modèle conventionnel de liste d'inclusion et de consentement. L'utilisation répandue des dispositifs d'identification des fréquences radio, de la nanotechnologie et des dépôts massifs de données qui appuient les nouveaux services du Web 2.0 soulèvent de sérieuses questions sur l'efficacité de la loi canadienne sur la protection des renseignements personnels.

Les gouvernements doivent également travailler avec le secteur privé pour élaborer des **solutions de gestion d'identité** qui permettent aux individus d'avoir une plus grande mainmise sur leurs renseignements personnels et leurs identités en ligne. Vecteur de commerce et de communication en pleine essor, Internet pose des défis qui sont moins dominants dans le monde hors ligne, particulièrement dans le domaine de la gestion d'identité. Par conséquent, les responsables canadiens de l'élaboration de politiques ont visé à élaborer des principes pour l'authentification électronique, alors que de nombreux systèmes ont été mis au point pour essayer de régler la difficulté d'identifier, en toute sécurité, les parties en ligne. Parmi les initiatives d'avant-garde, mentionnons le système CardSpace de Microsoft, qui permet aux utilisateurs de créer leur propre profil d'identité à l'aide de 15 champs d'information liée à l'identité. Le système permet également l'attribution d'une identité gérée à un fournisseur digne de confiance, comme une institution financière ou un employeur pour d'autres types de transactions.

Open ID, un système de gestion d'identité à l'intention des blogueurs et d'autres forums de discussion en ligne, est une solution à libre source qui attire environ 75 millions d'utilisateurs sur des sites populaires, tels que Technorati et LiveJournal. Il offre un

mécanisme relativement continu destiné à gérer l'identité personnelle dans les environnements en ligne, sans être obligé de créer et d'utiliser de multiples profils de connexion pour divers sites. Le besoin de solutions similaires à Open ID a été mis en évidence par le manque d'interopérabilité entre les sites de réseautage social populaires, ce qui signifie que les internautes doivent sans cesse rentrer leurs renseignements personnels pour chaque nouveau réseau auquel ils se joignent. Ils trouvent que chaque réseau est effectivement un « jardin clôturé », où les avantages du réseau sont artificiellement limités par l'incapacité de relier, par exemple, un ami sur Facebook avec un autre sur MySpace.

Certains gouvernements jouent également un rôle actif dans l'élaboration de solutions de gestion d'identité. Par exemple, le gouvernement sud-coréen a créé le i-NIP, qui remplace le besoin de divulguer des renseignements d'identité nationale. En règle générale, les utilisateurs peuvent le recevoir une fois que leur identité a été authentifiée par un numéro de carte de crédit, un message SMS ou en se présentant dans un bureau gouvernemental. Ce numéro d'identification personnelle facilite les transactions en ligne, car il authentifie le statut de citoyenneté d'une personne sans divulguer des éléments d'identification, comme le nom, la date de naissance ou le sexe.

Combattre les menaces sur Internet : pourriel, hameçonnage, logiciels espions et programmes nuisibles

Il y a plus de deux ans, le Groupe de travail du Canada sur le pourriel avait présenté au ministre de l'Industrie de l'époque, David Emerson, son rapport sur la façon dont Ottawa pourrait aider à lutter contre le pourriel (l'auteur du présent document faisait partie du Groupe de travail). À cette époque, le Canada n'était pas doté d'une **loi nationale anti-pourriel** et était considéré comme l'un des six plus grands pays polluposteurs au monde. De plus, la réponse divergente des fournisseurs de services Internet du Canada – certains avaient adopté des mesures dynamiques pour bloquer et filtrer les pourriels, alors que d'autres n'avaient guère pris de mesures pour endiguer la marée croissante de pourriels sortant de leurs réseaux – constituait une source de préoccupation supplémentaire. On peut presque pardonner les observateurs d'avoir cru que le problème du pourriel avait disparu. D'une part, les filtres anti-pourriel, qui sont devenus de plus en plus efficaces, limitent la quantité de pourriels qui entrent dans les boîtes de réception des utilisateurs; d'autre part, les FSI canadiens réussissent tellement bien à bloquer les pourriels avant qu'ils quittent leurs réseaux que le Canada ne figure plus dans la liste de la douzaine de pays les plus polluposteurs.

Malgré les réussites sur le front technique, les premières impressions peuvent être décevantes. Le volume mondial de pourriels continue d'augmenter; en effet, les récents sondages indiquent que 80 % de l'ensemble des courriels sont des pourriels. Les pourriels sont également devenus plus dangereux car de nombreux messages contiennent secrètement des virus ou d'autres programmes cachés qui peuvent transformer de simples

internauts ayant des connexions à large bande en des polluposteurs à grande échelle et ce, à leur insu. Les polluposteurs ont accentué le problème, car ils ne se limitent plus au courriel commercial non sollicité traditionnel. Des millions de blogues ont été touchés par des pourriels, appelés « splogues »; la téléphonie Internet fait également face à un problème croissant de pourriels, désignés par « spit »; et les courriels d’hameçonnage, qui renvoient les utilisateurs à des sites Web usurpés afin d’extraire leurs renseignements personnels, sont responsables des centaines d’incidents de vol d’identité.

L’effet cumulatif de cette activité peut être dévastateur pour la confiance des consommateurs et des entreprises, à mesure que ces derniers doutent de plus en plus de la légitimité du commerce en ligne et que les avantages économiques promis sont entravés par une largeur de bande bloquée par un trafic de courriels non voulus. Par exemple, selon une étude menée par le Groupe Gartner en 2005, 80 % des répondants avaient indiqué que les attaques en ligne avaient influé sur leur confiance à l’égard des courriels envoyés par des entreprises ou des individus qu’ils ne connaissent pas. De ce chiffre, plus de 85 % suppriment les courriels suspects, sans même les ouvrir, une pratique qui a de graves conséquences pour les banques et les entreprises qui souhaitent utiliser le courriel pour communiquer de façon plus rentable avec les clients. En outre, d’importants coûts sont en jeu car les FSI font face à des frais accrus – dont un bon nombre sont apparemment relégués aux consommateurs – pour traiter les volumes croissants de pourriels et déployer des technologies de filtrage anti-pourriel.

Malheureusement, le cadre juridique canadien n’a pas gardé le rythme avec les nouvelles préoccupations liées aux pourriels. Bien que le Canada maintienne sa position, de nombreux pays, dont la Nouvelle-Zélande, Hong Kong et le Japon, ont adopté de nouvelles lois pour combattre le pourriel, l’hameçonnage et les logiciels espions. Le besoin pour de telles lois est devenu particulièrement important à la lumière de la priorité accrue accordée à **l’application transfrontalière de mesures contre les menaces sur Internet**. Les polluposteurs et les hameçonneurs utilisent des ordinateurs dans plusieurs pays pour envoyer leur courriel et tentent d’effacer leurs traces en transférant leurs profits par le biais de multiples juridictions. Même si le Canada a participé à un dialogue mondial sur l’application, l’absence d’une loi exhaustive pourrait entraver la capacité des autorités de combattre les activités de pourriel, d’hameçonnage et de logiciels espions qui comportent un élément canadien.

Vers un cadre efficace de cybersécurité

Dans la foulée des événements du 11 septembre, tous les gouvernements ont rapidement pris des mesures pour évaluer leurs besoins en sécurité nationale. L’évaluation canadienne a abouti à un rapport intitulé *Protéger une société ouverte : la politique canadienne de sécurité nationale*. Premier document en son genre, ce rapport renfermait un plan détaillé pour contrer les menaces futures à la sécurité. Le rapport avait spécifiquement cerné la **cybersécurité** comme une question d’infrastructure essentielle, comme en témoigne le passage suivant : « La menace de cyberattaques est réelle, et les conséquences de telles attaques peuvent être graves. » Le rapport prenait l’engagement

d'améliorer considérablement l'analyse de la vulnérabilité des infrastructures Internet du Canada, ainsi que de renforcer sa capacité de défendre ses réseaux et de répondre aux cyberattaques.

Les préoccupations liées aux cyberattaques ont été intensifiées par le récent incident en Estonie, qui a paralysé l'infrastructure d'information et les transactions bancaires en ligne du pays. De plus, selon les récentes estimations de Google, parmi les 4,5 millions de pages Web, 700 000 contiennent des codes nuisibles qui pourraient compromettre un système d'information; de ce chiffre, 450 000 sites sont capables de lancer des téléchargements nuisibles. Bien des pays ont réagi à ces menaces par l'adoption de nouvelles lois. Par exemple, l'Allemagne a édicté une loi anti-cybercriminalité qui définit le piratage informatique comme l'acte de pénétrer un système de sécurité informatique et d'accéder à des données protégées, sans nécessairement les voler. La loi définit les contrevenants comme toute personne ou tout groupe qui crée, diffuse ou achète sciemment des outils de piratage conçu à des fins illégales.

De toute évidence, il est nécessaire que le développement d'une infrastructure de cybersécurité renforce la confiance de toutes les parties intéressées en incluant une représentation des groupes de protection de la vie privée et des droits civils. La sécurité est une valeur primordiale, mais elle doit respecter pleinement la vie privée et les droits civils de tous les Canadiens. En effet, les cas de surveillance répandue des communications téléphoniques aux États-Unis – souvent avec la participation secrète active d'entreprises de télécommunications –, ont fourni beaucoup de preuves qui démontrent le danger de se concentrer sur la sécurité, sans la contrebalancer avec la perspective de la vie privée et des droits civils.

Par ailleurs, on ne devrait pas considérer la priorisation de la cybersécurité comme un mécanisme facile pour promouvoir le programme de « l'accès légitime », qui pourrait obliger les fournisseurs de services Internet à installer de nouvelles fonctions d'interceptions dans leurs systèmes pour pouvoir saisir des données et identifier les activités particulières des abonnés. En réalité, les dispositions qui renforcent des activités de surveillance risquent de nuire à la confiance des Canadiens qui craindront que cela donne lieu à des surveillances indésirables sans une supervision appropriée.