Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner Of Canada

Document de consultation sur les renseignements concernant les noms et les adresses des clients

Réponse du Commissariat à la protection de la vie privée du Canada à la Sécurité publique Canada

Octobre 2007
Ottawa, Ontario

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

Raison d'être de la consultation

Selon le document de consultation publié par Sécurité publique Canada et Industrie Canada, « [l]es objectifs de ce processus visent à maintenir l'accès légal pour les organismes responsables de l'application de la loi et de la sécurité nationale dans le contexte du développement constant de nouvelles technologies, tout en préservant et en assurant la protection de la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada[1] ».

Le document de consultation se fonde sur l'hypothèse selon laquelle il est difficile pour les organismes responsables de l'application de la loi et de la sécurité nationale d'accéder à l'information sur les noms et adresses des clients de façon opportune. Le document de consultation énonce le problème de la manière suivante :

> Il est difficile pour les organismes d'application de la loi d'obtenir des fournisseurs de services de télécommunication, de façon constante, l'information de base sur les noms et adresses des clients. Sans dispositions législatives explicites, les différents fournisseurs de services de télécommunication observent toute une gamme de pratiques en ce qui a trait à la divulgation de l'information de base sur le client, notamment le nom, l'adresse, le numéro de téléphone ou leurs équivalents sur Internet. Certaines entreprises divulguent volontairement cette information, alors que d'autres exigent qu'un mandat soit présenté avant de fournir l'information demandée, quelle que soit la nature de cette information ou le contexte entourant la demande. Si le gardien de l'information refuse de coopérer lorsqu'une demande est faite pour obtenir cette information, les organismes chargés de faire appliquer la loi n'ont aucun moyen d'exiger la production des renseignements relatifs au client, ce qui peut poser un problème dans certains cas. Par exemple, les organismes d'application de la loi peuvent avoir besoin de l'information pour des raisons non reliées à une enquête (c.-à-d. pour trouver le plus proche parent en cas d'urgence) ou parce qu'il s'agit d'un début d'enquête. Le fait d'avoir accès à cette information de base constitue souvent la différence entre le début d'une enquête ou sa fin.

L'extrait ci-dessus donne à penser qu'il s'agit d'un problème d'incohérence; certains fournisseurs de services de télécommunication (FST) communiquent cette information de façon volontaire tandis que d'autres refusent ou n'acceptent de le faire que sur présentation d'un mandat.

Le document de consultation affirme que cette situation « peut poser problème dans certains cas » et fait référence à deux exemples où des problèmes peuvent survenir. Le premier implique le recours à l'information sur les noms et adresses des clients pour des raisons d'urgence non liées à une enquête, tandis que le

[1] Le document de consultation est disponible à l'adresse http://securitepublique.gc.ca/prg/ns/cna-fr.asp.

second implique l'utilisation de cette information au cours des premières étapes d'une enquête.

Malheureusement, le document de consultation ne fournit aucune indication quant à l'étendue des difficultés qui y sont mentionnées. Les FST transmettent-ils volontairement l'information sur les noms et adresses des clients selon une proportion de 80 %, ou est-ce que les chiffres sont plutôt de l'ordre de 20 %? Les compagnies de téléphone sont-elles plus susceptibles de fournir les renseignements que les fournisseurs de services Internet (FSI)? Les petits FST sont-ils plus susceptibles d'exiger un mandat? Le document de consultation n'indique pas non plus si les FST réagissent différemment selon la situation. Par exemple, les FST réagissent-ils différemment lorsqu'il s'agit de trouver le plus proche parent en cas d'urgence que lorsque les demandes ont trait à des crimes violents présumés?

Le fait d'exiger de tous les FST qu'ils communiquent sur demande l'information sur les noms et adresses des clients constitue une solution unique trop large à un problème qui n'a pas été clairement défini ou mesuré. Nous avons soulevé ce problème à la suite des consultations de 2002 et 2005 sur l'accès légal :

> Lorsqu'en 2002, le ministère de la Justice, Industrie Canada et le ministère du Solliciteur général ont fait paraître le *Document de consultation sur l'accès légal*, le Commissariat et plusieurs autres parties ont remis en question la nécessité de réviser le régime actuel d'accès légal. Nous avons fait remarquer que ces ministères n'avaient pas réussi à faire la preuve de l'existence d'un grave problème à régler. Nous leur avons enjoint de présenter un énoncé clair des problèmes que connaissaient les organismes d'application de la loi de même que des éléments de preuve empiriques à l'appui de la nécessité d'accroître les pouvoirs de surveillance comme le proposait le document de consultation.
>
> Ces ministères n'ont toujours pas donné suite à cette requête. Sans une compréhension claire des problèmes que le projet de loi doit résoudre, il est impossible pour le Commissariat et le public canadien de déterminer si les mesures proposées sont nécessaires et appropriées.

Bien que la consultation actuelle ne traite que de quelques-uns des problèmes soulevés au cours des consultations précédentes, les commentaires émis en 2005 sont toujours pertinents.

***Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*)**

Au même titre que les installations, ouvrages, entreprises ou secteurs d'activité fédéraux (entreprises fédérales), tous les FST qui exercent leurs activités au

Canada sont assujettis à la *LPRPDÉ*, même s'ils offrent uniquement leurs services au sein d'une province dotée de lois essentiellement similaires.

La *LPRPDÉ* exige que les organisations obtiennent un consentement pour la communication de renseignements personnels, sous réserve d'un nombre limité d'exceptions. Trois d'entre elles revêtent une pertinence particulière relativement aux problèmes soulevés dans le document de consultation :

- en vertu de l'alinéa 7(3)*c*), l'organisation peut communiquer un renseignement sans le consentement de l'intéressé lorsqu'elle est tenue de se conformer à une assignation, un mandat ou une ordonnance d'un tribunal;
- en vertu de l'alinéa 7(3)*c*.1), l'organisation peut communiquer un renseignement personnel à une institution gouvernementale, y compris un organisme d'application de la loi, aux fins du contrôle de l'application de la loi, de la tenue d'une enquête, de la collecte de renseignements en vue du contrôle d'application de la loi ou de l'application du droit;
- l'alinéa 7(3)*e*) permet la communication sans le consentement à toute personne qui a besoin du renseignement en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de toute personne.

L'alinéa 7(3)*c*) traite de la communication obligatoire aux termes d'une autorisation légale.

En revanche, l'alinéa 7(3)*c*.1) vise clairement à permettre aux organisations de communiquer des renseignements personnels sans consentement ni notification aux organismes responsables de l'application de la loi et de la sécurité nationale et autres organisations gouvernementales en l'absence d'une autorisation judiciaire préalable. Toutefois, l'organisme qui demande le renseignement doit faire part de son autorité juridique et mentionner qu'il recueille l'information pour l'une ou l'autre des raisons énumérées à l'alinéa, par exemple aux fins du contrôle d'application du droit canadien, provincial ou étranger.

Dans le cadre des délibérations à la Chambre des communes au sujet de la loi (projet de loi C-6), le ministre de l'Industrie a clairement énoncé que l'alinéa 7(3)*c*.1) visait à maintenir le *statu quo* : « Ces amendements ne confèrent aucun nouveau pouvoir aux institutions gouvernementales et ils n'imposent aucune nouvelle obligation aux entreprises. » Bien que l'alinéa 7(3)*c*.1) ne visait pas à modifier le *statu quo*, nous reconnaissons qu'il a pu créer une incertitude au sein des organisations qui se voient demander de communiquer certains renseignements.

Cette disposition a fait l'objet d'un nombre important de discussions au cours de la révision quinquennale obligatoire de la *LPRPDÉ* réalisée par le Comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique. Dans son rapport déposé le 2 mai 2007, le Comité a recommandé que soit étudiée la possibilité de clarifier le sens de l'expression « autorité légitime » à l'alinéa 7(3)*c*.1). Il a également recommandé de

remplacer le terme « peut » de l'alinéa liminaire du paragraphe 7(3) par le terme « doit », ce qui aurait apparemment rendu obligatoires toutes les communications présentées au paragraphe 7(3).

Dans sa réponse au rapport du Comité déposée le 17 octobre 2007, le gouvernement a fait état du besoin de clarifier le concept d'autorité légitime. Il a rejeté la recommandation du Comité voulant que le terme « peut » soit remplacé par le terme « doit ».

La réponse du gouvernement visait également à clarifier l'intention générale de l'alinéa :

> Le gouvernement souhaite confirmer que l'alinéa 7(3)*c*.1) a pour objet de permettre aux organisations de collaborer avec les organismes d'application de la loi et de sécurité nationale, sans nécessiter une assignation, un mandat ou une ordonnance des tribunaux. Les organisations qui partagent des renseignements avec les institutions gouvernementales, y compris les organismes d'application de la loi et de sécurité nationale, conformément aux exigences de cette disposition, agissent en conformité avec la *LPRPDÉ*.

Le gouvernement a également fait savoir qu'il étudierait la possibilité d'ajouter un règlement en vue de définir plus clairement le terme « institution gouvernementale » des alinéas 7(3)*c*.1) et 7(3)*d*).

Malgré que ni le rapport du Comité ni la réponse du gouvernement ne réfère directement à l'alinéa 7(3)*e*), dans sa réponse, le gouvernement énonçait qu'il songerait à certaines exceptions limitées aux exigences de la *LPRPDÉ* relatives au consentement afin de traiter des préoccupations soulevées par les intervenants quant à la communication de renseignements personnels en cas de désastre naturel, de violence faite aux aînés et dans d'autres circonstances similaires. Un tel changement s'avérerait sans aucun doute pertinent en matière de communication de l'information sur les noms et adresses de clients aux organismes responsables de l'application de la loi et de la sécurité nationale en cas de situations urgentes.

Comme le laisse entendre le document de consultation, l'incohérence fait partie des difficultés rencontrées par les organismes responsables de l'application de la loi et de la sécurité nationale au moment d'obtenir l'information sur les noms et adresses des clients. Les modifications que propose d'apporter le gouvernement à la *LPRPDÉ* aux termes de la révision quinquennale devraient bien clarifier le moment et la façon dont les FST peuvent communiquer l'information sur les noms et adresses des clients en vertu de l'alinéa 7(3)*c*.1) et éventuellement de l'alinéa 7(3)*e*).

La commissaire à la protection de la vie privée a affirmé publiquement qu'elle ne s'objectait pas à l'ajout de la définition des termes « autorité légitime » et « institution gouvernementale » si le gouvernement était d'avis que de telles définitions clarifieraient la loi.

Bien que le document de consultation désigne l'absence de dispositions législatives explicites à titre de problème que tente de régler le processus de consultation, la *LPRPDÉ* constitue en fait un code législatif explicite qui donne un accès légal aux organismes responsables de l'application de la loi et de la sécurité nationale tout en « préservant et en assurant la protection de la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada. » Avant de songer à établir des lois qui rendraient obligatoire la communication sur demande de l'information sur les noms et adresses des clients, nous recommandons fortement que le gouvernement détermine si la clarification de la *LPRPDÉ* mentionnée ci-dessus, accompagnée de lignes directrices appropriées, pourrait régler le problème d'incohérence. En ce qui a trait aux lignes directrices, Service Alberta a produit un document d'orientation intitulé *Requesting Personal Information from the Private Sector: Forms and Guidelines for Law Enforcement Agencies*, qui présente deux formulaires dont peuvent se servir les organismes d'application de la loi au moment de demander un renseignement personnel à une organisation[2].

Noms et adresses des clients et attente en matière de protection de la vie privée

Le document de consultation ne définit pas l'information sur les noms et adresses des clients, mais il énonce qu'elle pourrait comprendre « les identificateurs de base suivants » :

- nom;
- adresse(s);
- numéro de téléphone de dix chiffres (service conventionnel à fil ou service sans fil);
- identificateurs de téléphone cellulaire, c.-à-d. un ou plusieurs identificateurs uniques associés à un abonné d'un service particulier de télécommunication (numéro d'identification de service mobile; numéro de série électronique; identité internationale d'équipement mobile; identité internationale d'abonné mobile; numéro de carte de module d'identité d'abonné ou numéro de carte SIM);
- adresse(s) de courriel;
- adresses IP;
- identificateur du fournisseur de services locaux, c.-à-d. identification du fournisseur de services de télécommunication à qui appartient le numéro de téléphone ou l'adresse IP dont se sert un client en particulier.

Il s'avère trompeur de faire référence à tous ces renseignements en tant qu'information sur les noms et adresses des clients, tout comme de nommer « identificateurs de base » ces éléments de données. Cette liste va bien au-delà des noms et adresses du consommateur associés à un numéro de téléphone donné. Certains de ces renseignements sont accessibles par l'entremise des

[2] Voir http://www.pipa.gov.ab.ca/resources/pdf/forms_and_guidelines_for_law_agencies.pdf.

annuaires de pages blanches et des annuaires par numéros. Toutefois, la plupart d'entre eux ne sont pas accessibles au public; en outre, bon nombre seraient inconnus des personnes en cause. Par exemple, bien des gens dotés d'un accès Internet ne connaissent pas leur adresse IP. Parallèlement, beaucoup d'abonnés au téléphone cellulaire ne savent même pas qu'il existe des identificateurs associés à leur téléphone autre que le numéro.

L'hypothèse qui sous-tend le document de consultation est que l'information sur les noms et adresses des clients comporte de faibles attentes quant à la protection de la vie privée et, qu'à ce titre, ne nécessite aucune autorisation judiciaire. Nous ne sommes pas d'accord. En effet, bien des gens considèrent la plupart de ces renseignements comme privés. D'abord, un grand nombre de personnes choisissent de payer un supplément pour des numéros non inscrits à l'annuaire, montrant qu'elles les jugent privés. Beaucoup partagent leurs numéros de téléphone cellulaire uniquement avec leurs parents et amis. L'un des attraits d'Internet est qu'il offre une attente en matière de protection de la vie privée. Nombreux sont ceux qui utilisent un pseudonyme en vue d'entretenir des communications anonymes ou pour une foule d'autres raisons[3].

Dans l'arrêt *BMG et al c. John Doe et al*, le juge von Finckenstein a conclu qu'il serait irresponsable de la part de la Cour d'ordonner la communication du nom d'un détenteur de compte en raison de l'incertitude qui existe quant au lien entre l'identité d'un détenteur de compte et un utilisateur anonyme ainsi que le lien entre l'utilisateur d'un compte et une adresse IP active donnée[4].

Bien que certains de ces renseignements puissent être jugés moins sensibles, il nous faut admettre qu'ils ne sont pas généralement recherchés comme une fin en soi. L'information sur les noms et adresses des clients peut être utile aux organismes responsables de l'application de la loi et de la sécurité nationale particulièrement parce qu'elle est susceptible de leur donner accès à des renseignements encore plus sensibles.

L'article 8 de la *Charte canadienne des droits et libertés* protège la population contre des perquisitions et saisies abusives lorsqu'il existe une attente raisonnable

---

[3] Voir le juge Wilkins dans l'affaire *Irwin Toy Ltd. c. Doe* (2000), 12 C.P.C. (5e) 103 (C.S. Ont.) aux paragraphes 10-11 : [traduction] « La circulation des renseignements via Internet sous le couvert d'un nom d'emprunt ou d'un pseudonyme s'appuie implicitement sur une compréhension partagée du fait que l'identité de la source restera jusqu'à un certain point confidentielle. Certains prestataires de service Internet informent leurs clients qu'ils respecteront leur droit à la vie privée. Certains vont même jusqu'à procéder à l'examen de leur politique de protection de la vie privée et à en faire vérifier l'application. En général, il est entendu que l'adresse IP d'un client n'est pas communiquée. Il semble que certains prestataires de service Internet exigent que leurs clients s'engagent à ne pas envoyer de messages diffamatoires, et qu'ils prennent en contrepartie des mesures raisonnables pour préserver l'anonymat de la source de renseignements. »

[4] *BMG Canada Inc. c. John Doe* [2004] 3 R.C.F. 241.

en matière de protection de la vie privée. La Cour suprême a reconnu que l'attente de quiconque à cet effet peut dépendre de l'endroit, de la nature du renseignement de même que du lien qui l'unit à la personne concernée. Au sujet du troisième point, afin de trancher sur le caractère raisonnable de l'attente d'une personne en matière de protection de la vie privée, la Cour cherche à savoir si les renseignements personnels impliquent « un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démocratique, vouloir constituer et soustraire à la connaissance de l'État[5]. »

Dans l'arrêt *R. c. Plant*, où le concept d'« ensemble de renseignements biographiques d'ordre personnel » a été employé pour la première fois, la Cour a jugé que les dossiers de consommation d'électricité ne passaient pas le test de renseignements biographiques. Pour tirer cette conclusion, la Cour a tenu compte du fait que le public a généralement accès à ce genre de renseignements, contrairement aux numéros de téléphones résidentiels et cellulaires non inscrits à l'annuaire que protègent farouchement de nombreuses personnes, indiquant ainsi une attente élevée relative à la protection de la vie privée.

Dans un solide jugement dissident dans l'arrêt *R. c. Plant*, la juge McLachlin (tel était alors son titre) a noté ce qui suit :

> Les ordinateurs peuvent, et devraient, être des endroits privés, les données qui y sont emmagasinées bénéficiant de la protection juridique qu'entraîne une attente raisonnable quant au respect de la vie privée. Un ordinateur peut contenir une abondance de renseignements personnels qui, suivant leur nature, peuvent être tout aussi privés que ceux qui se trouvent dans une maison d'habitation ou dans une chambre d'hôtel[6].

Bon nombre des divers types de renseignements personnels, sinon leur totalité, compris dans la mal nommée catégorie de l'information sur les « noms et adresses des clients » constituent des renseignements personnels auxquels correspond une attente raisonnable en matière de protection de la vie privée. Nous recommandons fortement d'accorder l'attention voulue aux répercussions sur la *Charte* de toute loi qui obligerait les FST à communiquer ces renseignements personnels lorsqu'ils font face à une requête sans mandat qui s'avère, en réalité, une demande.

Mesures de sécurité proposées

Le document propose un certain nombre de mesures de sécurité qui pourraient être mises en œuvre si le gouvernement décide d'exiger des FST qu'ils communiquent, sur demande, l'information sur les noms et adresses des clients. Toutefois ces mesures deviennent pertinentes seulement si une personne accepte que la communication obligatoire constitue une solution appropriée et nécessaire.

[5] *R. c. Plant*, [1993] 3 R.C.S. 281.
[6] *Ibid.*, paragr. 45.

Nous ne nous proposons pas d'émettre des commentaires détaillés au sujet des mesures proposées. Nous ferons des remarques plus approfondies sur les freins et contrepoids de même que sur les modèles de surveillance advenant l'adoption d'une loi visant la mise en œuvre de ces propositions.

Le document de consultation suggère que les dirigeants des organismes soient tenus d'effectuer des vérifications internes régulières en vue d'assurer que toute demande d'obtention d'information sur les noms et adresses des clients soit présentée conformément aux protocoles et aux mesures de sécurité en place. Le document suggère également de soumettre les résultats des vérifications à la commissaire à la protection de la vie privée, au Comité de surveillance des activités de renseignement de sécurité ou à un commissaire provincial à la protection de la vie privée, comme il convient.

Le document fait aussi référence aux dispositions explicites permettant à la commissaire à la protection de la vie privée et au Comité de surveillance des activités de renseignement de sécurité d'effectuer des vérifications portant sur la diffusion de l'information sur les noms et adresses des clients.

Bien que les vérifications après le fait s'avèrent un moyen important d'évaluer la conformité, elles ne remplacent pas les autorisations préalables. En ce qui a trait à notre capacité à effectuer des vérifications concernant la communication de l'information sur les noms et adresses des clients, le Commissariat peut, à tout moment, analyser la conformité d'un ministère ou d'un organisme du gouvernement à la discrétion de la commissaire en application de l'article 37 de la *Loi sur la protection des renseignements personnels.* En vertu de l'article 18 de la *LPRPDÉ*, nous exigeons qu'il y ait des « motifs raisonnables de croire » qu'une organisation contrevient à la Loi avant que nous puissions effectuer une vérification. Bien que certains commissaires provinciaux soient habilités à mener des vérifications auprès d'un service policier provincial ou municipal pour ce qui est de la conformité avec les lois provinciales portant sur la protection de la vie privée, ils n'ont pas tous le pouvoir ou les ressources pour effectuer un tel examen. Il est difficile de voir de quelle façon le gouvernement fédéral pourrait obliger un service de police provincial ou municipal à conserver les dossiers de vérification. Une importante lacune sur le plan de la surveillance découlerait possiblement de cette situation.

Conclusion

Le document de consultation est fondé sur un ensemble d'hypothèses, notamment les suivantes :

1. Les organismes responsables de l'application de la loi et de la sécurité nationale éprouvent des difficultés à accéder à l'information sur les noms et adresses des clients qui sont suffisamment graves pour justifier de nouvelles mesures portant atteinte à la protection de la vie privée.
2. Il n'existe aucune attente raisonnable en matière de protection de la vie privée dans les données sur les noms et adresses des clients.

3. Il s'avère nécessaire d'obliger les FST à communiquer ces renseignements sur demande en vue d'enrayer ces problèmes.
4. Cette approche préserve et protège « la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada », comme le laisse entendre le document de consultation.

Nous doutons de la solidité de ces hypothèses. Premièrement, nous n'avons pas une vision claire de la gravité du problème. Ni ce document de consultation ni les précédents n'ont présenté de justification, fondée sur des preuves empiriques, que l'incapacité d'obtenir les noms et adresses des clients de manière opportune avait causé de graves problèmes aux organismes responsables de l'application de la loi et de la sécurité nationale au Canada. Cette situation met en doute la justification de la politique du point de vue de la proportionnalité et de la nécessité. Deuxièmement, nous sommes d'avis qu'une attente raisonnable concernant la protection de la vie privée se rattache aux données sur les noms et adresses des clients. Cela met en doute la validité constitutionnelle de tout régime de communication ou de perquisition obligatoire.

En prenant pour acquis l'existence d'un problème bien documenté et prouvé empiriquement quant à l'obtention d'un accès à l'information sur les noms et adresses des clients, nous ne sommes pas convaincus que le fait d'exiger des FST qu'ils communiquent cette information sans mandat constitue la seule solution ou du moins la solution la plus appropriée. Comme il a été discuté ci-dessus, la clarification de la *LPRPDÉ* et l'offre de directives peuvent s'avérer fort utiles dans la résolution de ce problème. Nous soulignons également que le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a déjà réglé la question de l'accès aux renseignements détenus par les fournisseurs (IFSL) grâce à des organismes d'application de la loi dans la décision de télécom CRTC 2002-21[7]. Dans sa décision, le CRTC a déterminé que, pour obtenir l'identité du fournisseur de services locaux (IFSL), un organisme d'application de la loi devait identifier la source de l'autorité légitime lui permettant d'obtenir l'information et indiquer ce qui suit :

1. qu'il a des motifs raisonnables de croire que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;
2. que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application;
3. que la communication est faite en raison d'une situation d'urgence menaçant la vie, la santé ou la sécurité de toute personne, ou afin de permettre à un

[7] Décision de télécom CRTC 2002-21, 12 avril 2002, Fourniture aux organismes d'application de la loi de renseignements sur l'identité des fournisseurs de services de télécommunication des abonnés.

> organisme d'application de la loi de remplir ses obligations afin d'assurer la protection et la sécurité des personnes et de la propriété.

Le langage utilisé dans la décision du CRTC est similaire à celui du paragraphe 7(3) de la *LPRPDÉ* avec l'ajout significatif de la référence à l'expression « motifs raisonnables de croire ». L'approche du CRTC devrait également être prise en compte.

Enfin, nous sommes d'accord avec le document de consultation à l'effet que « [l]es principes et les pouvoirs relatifs à l'accès légal doivent être exercés de façon à respecter les droits et les libertés garantis par la *Charte canadienne des droits et libertés* ». Toutefois, nous doutons que le fait de permettre aux organismes responsables de l'application de la loi et de la sécurité nationale d'obtenir sur demande l'information sur les noms et adresses des clients satisferait cette exigence. Comme il a été mentionné précédemment, nous n'acceptons par la prémisse voulant que les personnes aient une faible attente en matière de protection de la vie privée et que l'obtention de cette information sans autorisation judiciaire protégerait « la vie privée ainsi que les autres droits et libertés de toutes les personnes habitant au Canada ».