PAR COURRIEL
ic.telecomsubmission-soumissiontelecom.ic@canada.ca

Montréal, le 8 avril 2019

Madame Pamela Miller
Directrice générale
Direction générale des politiques sur Internet
et les télécommunications
Innovation, Sciences et Développement économique Canada
10e étage, 235 rue Queen
Ottawa (Ontario) K1A 0H5

Objet : Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation

Madame,

1. Le Conseil provincial du secteur des communications (CPSC) du Syndicat canadien de la fonction publique (SCFP) représente plus de 7300 personnes travaillant dans le secteur des télécommunications et des médias au Québec. Par la présente, il souhaite transmettre à Innovation, Sciences et Développement économique Canada ses observations sur le projet de *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation*.

2. Ce projet de décret a été publié dans la Gazette du Canada, partie 1[1], le 9 mars 2019. Il vise à donner au CRTC l'obligation de prendre davantage en compte certains éléments de la politique canadienne de télécommunication[2] dans ses politiques et décisions.

[1] Gazette du Canada, Partie 1, *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation,* vol. 153, no 10, p. 853 à 860.
[2] *Loi sur les télécommunications*, art. 7.

3. Ces nouvelles instructions d'application générale sont jugées pertinentes et nécessaires parce que les services de télécommunication sont maintenant des piliers de base de l'économie et de la société[3]. Le gouvernement spécifie que :

> « L'accès à des services de télécommunication de qualité et l'abordabilité de ces services sont de plus en plus importants pour permettre aux Canadiens de participer à l'économie numérique et à la société et y prospérer, et jouent un rôle fondamental dans la durabilité et le renforcement de la compétitivité du Canada dans l'économie mondiale. […] Le gouvernement se préoccupe des résultats pour les consommateurs dans le secteur des télécommunications au chapitre de la concurrence, de l'abordabilité, du choix, de la protection des consommateurs et de l'innovation des offres de service[4]. »

4. Ce sont des objectifs louables, présentés comme les priorités du gouvernement. Les passages soulignés dans la politique canadienne de télécommunication reproduite ci-dessous sont renforcés par le projet de décret :

> **7** La présente loi affirme le caractère essentiel des télécommunications pour l'identité et la souveraineté canadiennes; la politique canadienne de télécommunication vise à :
>
> **a)** favoriser le développement ordonné des télécommunications partout au Canada en un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions;
>
> **b)** permettre l'accès aux Canadiens dans toutes les régions — rurales ou urbaines — du Canada à des services de télécommunication sûrs, abordables et de qualité;
>
> **c)** accroître l'efficacité et la compétitivité, sur les plans national et international, des télécommunications canadiennes;
>
> **d)** promouvoir l'accession à la propriété des entreprises canadiennes, et à leur contrôle, par des Canadiens;
>
> **e)** promouvoir l'utilisation d'installations de transmission canadiennes pour les télécommunications à l'intérieur du Canada et à destination ou en provenance de l'étranger;
>
> **f)** favoriser le libre jeu du marché en ce qui concerne la fourniture de services de télécommunication et assurer l'efficacité de la réglementation, dans le cas où celle-ci est nécessaire;
>
> **g)** stimuler la recherche et le développement au Canada dans le domaine des télécommunications ainsi que l'innovation en ce qui touche la fourniture de services dans ce domaine;
>
> **h)** satisfaire les exigences économiques et sociales des usagers des services de télécommunication;
>
> **i)** contribuer à la protection de la vie privée des personnes.

---

[3] Gazette du Canada, Partie 1, *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation,* vol. 153, nº 10, p. 856.

[4] *Ibidem*, p. 853.

Pour des services de télécommunication sûrs

5. Dans le contexte actuel d'effervescence technologique – avec l'arrivée prochaine de la transmission cellulaire 5G qui rendra usuelle l'utilisation de l'intelligence artificielle et de données massives, entre autres –, le CPSC s'explique cependant mal que la sûreté des télécommunications soit le seul élément de la clause 7b) à ne pas être renforcé par le projet de décret. Ce dernier prévoit en effet que :

> « 1. Dans l'exercice des pouvoirs et fonctions qui lui confère la *Loi sur les télécommunications*, le Conseil met en œuvre la politique canadienne de télécommunication énoncée à l'article 7 de cette loi selon les principes suivants :
>
> a) lorsqu'il a recours à la réglementation, il devrait examiner comment les mesures prises peuvent promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation, notamment la mesure dans laquelle elles :
>
> (i) encouragent toute forme de concurrence,
> (ii) favorisent l'abordabilité et des prix plus bas, surtout lorsqu'il est possible que les fournisseurs de services de télécommunication soient en mesure d'exercer un pouvoir sur le marché,
> (iii) font en sorte qu'un accès abordable à des services de télécommunication de haute qualité soit disponible,
> (iv) renforcent et protègent les droits des consommateurs dans leurs relations avec les fournisseurs des services de télécommunications,
> (v) réduisent les barrières à l'entrée sur le marché et à la concurrence pour les nouveaux et les petits fournisseurs des services de télécommunications,
> (vi) permettent l'innovation dans les services de télécommunication, y compris de nouvelles technologies et des offres de services différenciées,
> (vii) stimulent l'investissement dans la recherche et le développement et dans d'autres actifs incorporels qui soutiennent l'offre et la fourniture de services de télécommunication;
>
> b) lorsqu'il a recours à la réglementation, il devrait démontrer sa conformité avec le présent décret et devrait préciser comment les mesures prises peuvent, selon le cas, promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation[5]. »

[notre soulignement]

6. Si le projet de décret est adopté tel quel, l'abordabilité et la qualité des services de télécommunication, la concurrence et l'innovation auront préséance sur la sûreté de ces mêmes services. Lorsqu'il adoptera une réglementation, le CRTC devra en effet démontrer qu'elle est conforme à ces objectifs, mais il n'aura toutefois aucune obligation de prouver qu'elle permet d'assurer la sécurité des réseaux de télécommunication.

[5] Gazette du Canada, Partie 1, *Décret donnant au CRTC des instructions relativement à la mise en œuvre de la politique canadienne de télécommunication pour promouvoir la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation,* vol. 153, nº 10, p. 860 et 861.

7. Pourtant, les technologies de l'information et de la communication font partie des dix secteurs d'infrastructures décrits dans la Stratégie nationale sur les infrastructures essentielles du gouvernement du Canada[6] :

> « On entend par infrastructures essentielles l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontières du pays. La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public[7]. »
>
> [notre soulignement]

8. Le fait que des fournisseurs de services de télécommunication (FST) font actuellement effectuer du travail sur les réseaux de télécommunication canadiens à des employés ou à des sous-traitants situés à l'extérieur du pays augmente les risques pour ces infrastructures essentielles. Telus sous-traite notamment du travail à des entreprises étrangères comme Tata qui gère depuis l'Inde l'ouverture de ports informatiques au Canada. Des travaux de support, de configuration d'équipements de réseaux et de conception de réseaux sont aussi confiés à des sous-traitants étrangers. Cela comporte des risques sécuritaires auxquels s'ajoutent des risques économiques puisqu'Internet est dorénavant utilisé dans le cadre des activités courantes d'une foule d'entreprises dans divers domaines.

9. Dans son Plan d'action 2018-2020 sur les infrastructures essentielles, le Forum national intersectoriel mis en place par Sécurité publique Canada reconnaît d'ailleurs que :

> « La convergence croissante des domaines virtuel et physique présente également de nouveaux défis pour les infrastructures essentielles du Canada. L'augmentation du recours aux services publics connectés, à l'automatisation et à l'intelligence artificielle, de même que la multiplication des appareils branchés, offre d'énormes possibilités aux secteurs des infrastructures essentielles et à l'économie canadienne puisque les technologies permettent des analyses plus rapides et contribuent à faire fonctionner les systèmes de façon plus efficace. Les services publics connectés intègrent les cybertechnologies et l'infrastructure physique pour améliorer l'efficacité des centres urbains au plan environnemental et économique, de même que la mobilité des personnes et des biens (p. ex. des réseaux électriques interconnectés pour réduire les pertes, des systèmes de transport plus intelligents et mieux synchronisés). Cependant, le fait que les organisations se fient de plus en plus aux cybersystèmes et aux technologies entraîne une exposition à de nouveaux risques qui pourraient avoir d'importantes conséquences physiques[8]. »
>
> [notre soulignement]

---

[6] Les dix secteurs d'infrastructures essentielles du gouvernement du Canada sont : la santé, l'eau, la sécurité, le secteur manufacturier, l'énergie et les services publics, les finances, l'alimentation, le transport, le gouvernement et les technologies de l'information.

[7] Gouvernement du Canada, *Stratégie nationale sur les infrastructures essentielles*, 2009, p. 2.

[8] Sécurité publique Canada, *Plan d'action 2018-2020 sur les infrastructures essentielles du Forum national intersectoriel*, 2018, p. 5.

10. En faisant primer l'abordabilité, la concurrence et l'innovation sur la sécurité des télécommunications, les instructions du gouvernement encourageront les FST à continuer d'avoir recours à des ressources situées à l'extérieur du pays pour réduire leurs coûts. Une pratique qui augmente aussi les risques de prises de contrôle politiques, de cyberterrorisme ou encore les risques reliés à des conflits ou à des catastrophes environnementales, etc[9]. Tous ces risques sont décuplés par la dépendance aux réseaux IP des autres infrastructures essentielles du pays (aéroports, banques, ports, services publics, hôpitaux, etc.) et de larges pans de l'économie canadienne[10]. Des partenariats avec des entreprises étrangères[11] ajoutent également aux dangers potentiels reliés aux services de télécommunication, ce dont le gouvernement est pleinement conscient.

11. Des notes de breffage préparées par Sécurité publique Canada en vue d'une rencontre des pays des « Five Eyes », en août dernier, mentionnent que le Canada « …« recognizes the risks associated with foreign equipment (4G and 5G) being deployed in Canadian telecommunications infrastructure, » including products built with backdoors to allow access to networks to disrupt systems, steal data and spy on businesses[12]. »

12. L'ampleur des menaces sécuritaires reliées à l'utilisation massive des réseaux de télécommunication justifie pleinement que le gouvernement ajoute la sécurité à ses priorités pour le système de télécommunication canadien. Le CPSC recommande donc l'ajout suivant (en gras) à l'alinéa 1a)(iii) de sa proposition de décret pour qu'il se lise comme suit :

    (iii) font en sorte qu'un accès abordable à des services de télécommunication de haute qualité **et sécuritaires** soit disponible.

Pour la création d'emplois au Canada

13. En donnant l'obligation au CRTC de s'assurer que sa réglementation favorise la sécurité des installations des FST, le gouvernement contribuerait par ailleurs à l'atteinte de deux autres objectifs de la politique canadienne de télécommunication.

14. Présentement, presque tous les grands FST réglementés par le CRTC font effectuer une partie plus ou moins importante de leurs opérations à l'extérieur du pays. En déplaçant des emplois hors du Canada, ils en évacuent la richesse, ce qui entre en contradiction avec la politique canadienne de télécommunication qui a notamment pour but de « … sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions[13]; »

---

[9] Dans son rapport annuel, Telus déclare aussi des « … risques reliés aux infrastructures et à la sécurité… », des « risques propres au pays (les différences et les changements à l'égard des régimes politiques, économiques et sociaux y compris les changements à l'égard des régimes juridiques et réglementaires), […] les risques liés aux catastrophes naturelles ainsi que le type de catastrophes et la fréquence à laquelle celles-ci se produisent; les fluctuations du change. » in : Telus, *Rapport annuel 2017,* p. 100.

[10] Le CRTC a fait des services à large bande des services de base en raison de leur caractère essentiel, in : CRTC, *Les services de télécommunication modernes : La voie d'avenir pour l'économie numérique canadienne,* Politique réglementaire de télécom CRTC 2016-496, Ottawa, 21 décembre 2016.

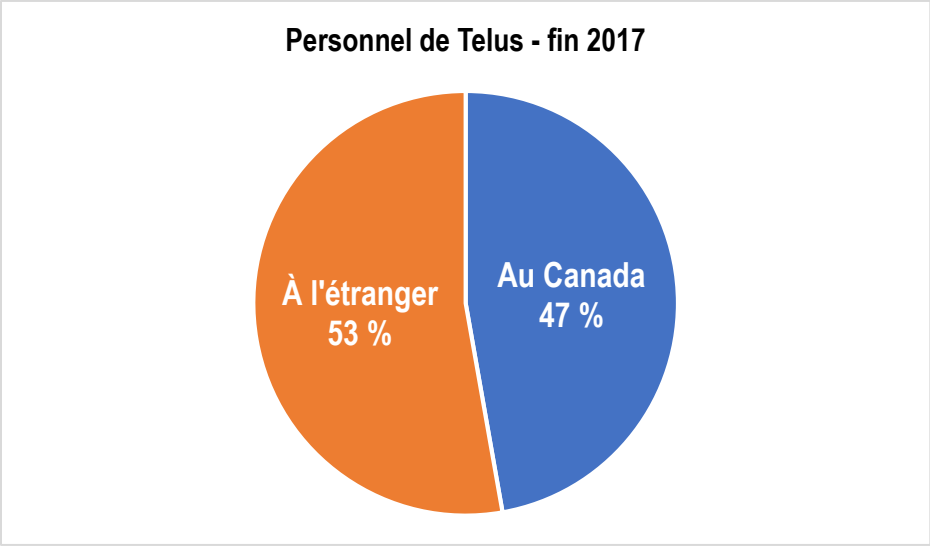
[11] Telus et Bell ont notamment un partenariat avec Huawei pour le développement de la technologie de transmission 5G : https://www.cbc.ca/news/business/bell-5g-network-plans-huawei-1.5009572 et https://www.cbc.ca/news/business/telus-huawei-earnings-1.5019946.

[12] Ahmad Hathout, *Gov't should encourage Canadian 5G equipment: Public Safety notes*, The Wire Report, April 1, 2019.

[13] *Loi sur les télécommunications*, art. 7a).

15. L'exemple le plus frappant à ce sujet est probablement celui de Telus qui déclare avoir des activités dans au moins dix pays : États-Unis, Irlande, Philippines, Roumanie, Bulgarie, Inde, Barbade, Salvador, Guatemala et Royaume-Uni[14]. Ses opérations à l'extérieur du Canada sont si importantes que l'entreprise emploie maintenant davantage de personnel à l'étranger qu'au pays.

TABLEAU 1 – Effectifs de Telus au Canada et ailleurs dans le monde



Source : Telus, *Rapport annuel 2017*.

16. Mettre la priorité sur la sécurité dans le décret d'instructions au CRTC permettrait donc de conserver ou de rapatrier des emplois au Canada, certaines opérations ne pouvant plus être sous-traitées à l'étranger sans comporter un risque supplémentaire pour les infrastructures essentielles de télécommunication canadiennes.

Pour la protection de la vie privée

17. Cela contribuerait également à renforcer la protection de la vie privée prévue à l'alinéa 7i) de la politique canadienne de télécommunication et à garantir par le fait même l'acceptabilité sociale des technologies de télécommunication innovantes citées à l'alinéa 1a)(vi) du décret proposé.

18. La technologie de transmission cellulaire 5G – dont les enchères du spectre sont prévues en 2020 – permettra l'avènement d'une multitude d'objets connectés et la généralisation de l'utilisation de l'intelligence artificielle, ce qui multipliera la quantité de données personnelles en circulation[15]. Cela entraînera son lot de risques pour la protection de la vie privée. On a qu'à penser à la domotique, à la reconnaissance faciale et aux équipements de la ville intelligente qui pourront suivre à la trace les activités des citoyens grâce aux infrastructures des FST.

19. Le CRTC reconnaît déjà en partie ces dangers. Il a entre autres commencé à prendre des mesures pour protéger les renseignements personnels des personnes faisant un appel d'urgence dans le cadre de sa

[14] Telus, *Rapport annuel 2017*, p. 12, 42 et 104.
[15] Tchéhouali, Destiny; Plamondon, Josée. (2018), *Données d'usage et usage des données à l'ère des plateformes : De la nécessité d'un encadrement réglementaire pour une meilleure affirmation de notre souveraineté numérique*, Montréal, ISOC Québec pour la Coalition pour la culture et les médias (CCM), p. 6 et 7.

réglementation des réseaux 9-1-1 de prochaine génération (9-1-1 PG). Autrefois entièrement sécurisés puisque sur fil de cuivre, les réseaux 9-1-1 sont graduellement remplacés par des systèmes fondés sur le protocole Internet. Ces derniers sont donc plus sensibles aux attaques informatiques, mais aussi potentiellement situés en partie en territoire américain (en raison de la configuration actuelle du réseau Internet), ce qui ajoute un risque lié à la juridiction.

20. Dans le cadre précis des services 9-1-1 PG, le CRTC a donc déterminé ce qui suit pour assurer la protection de la vie privée des Canadiens :

> « Afin d'assurer la sécurité des réseaux 9-1-1 PG et des renseignements transmis par ces réseaux, il est approprié que les réseaux 9-1-1 PG et tous les renseignements transmis par ceux-ci demeurent de compétence canadienne dans la plus grande mesure du possible.
>
> En conséquence, le Conseil impose une obligation, comme condition à l'offre et à la prestation de services de télécommunication aux termes de l'article 24 de la *Loi*, selon laquelle les fournisseurs de réseaux 9-1-1 PG doivent prendre toutes les mesures raisonnables pour assurer que toutes les composantes des réseaux 9-1-1 PG demeurent au Canada et que tout le trafic transitant par leurs réseaux 9-1-1 PG et destiné à un CASP[16] situé au Canada demeure au Canada. Si les fournisseurs de réseaux 9-1-1 PG souhaitent utiliser des composantes situées à l'extérieur du Canada, ils doivent en aviser le Conseil, en fournissant une justification exhaustive expliquant pourquoi il n'est pas raisonnable d'installer les composantes au Canada, dans un délai de six mois précédant l'utilisation proposée de ces composantes[17]. »
>
> [notre soulignement]

21. Le CRTC a estimé que des garanties contractuelles[18] ne suffisaient pas pour assurer le respect de la vie privée dans un environnement IP et il a imposé par sa réglementation une configuration de réseaux qui limite le trafic des données reliées aux appels d'urgence au territoire canadien.

22. Il faut dire que la juridiction dans laquelle se trouvent les données a son importance comme l'explique de façon éloquente une étude réalisée par l'Université de Toronto. Il y a en effet un risque pour la vie privée et les droits constitutionnels des Canadiennes et Canadiens qui va au-delà des simples problèmes de sécurité informatique lorsque leurs données transitent par un autre territoire – les États-Unis[19] par exemple.

> « *When Canadians store their data, for example, in the United States, their data can be accessed by United States government authorities on standards that would be unconstitutional if applied within Canada. Nor can Canadians expect that United States constitutional standards will apply*

---

[16] Centre d'appels de la sécurité publique.

[17] CRTC, Politique réglementaire de télécom CRTC 2017-182, *9-1-1 de prochaine génération – Modernisation des réseaux 9-1-1 afin de satisfaire aux besoins des Canadiens en matière de sécurité publique,* Ottawa, 1er juin 2017, par. 124 et 125.

[18] Le CRTC impose en plus aux fournisseurs de services de télécommunication d'élaborer des politiques de conservation et de destruction des informations personnelles et de garantir que toute donnée transmise dans le cadre des services d'urgence 9-1-1, par eux ou par un tiers, soit « … utilisée uniquement pour répondre aux communications liées au 9-1-1, à moins que l'abonné ne consente expressément à la divulgation ou à un autre usage ou que la divulgation soit ordonnée en vertu d'un pouvoir juridique. », *ibidem*, par. 232.

[19] Les données des Canadiens sont fréquemment entreposées aux États-Unis, car les communications par Internet ne restent pas sur le territoire canadien. Elles empruntent plutôt un parcours en zigzag des deux côtés de la frontière.

to them. Furthermore, specific US legislation explicitly provides a lower level of privacy protection to the digital data of non-US persons[20]. »

23. En vertu de la *USA's Foreign Intelligence Surveillance Act Amendments Act (FISAAA*), le gouvernement américain peut ainsi intercepter les données de tout citoyen étranger entreposées sur son sol et forcer les entreprises américaines à lui fournir les renseignements en leur possession sans révéler que ces informations ont été demandées[21]. La FISAAA permet donc l'accès à l'information personnelle de citoyens canadiens stockée aux États-Unis selon un standard différent de celui qui s'applique aux citoyens américains.

24. Par ailleurs, la jurisprudence américaine reconnaît la doctrine de la tierce partie[22]. Selon cette doctrine, les autorités américaines n'ont pas besoin de mandat pour accéder à de l'information qui a été partagée avec une tierce partie ou à laquelle une tierce partie a déjà accès[23]. C'est entre autres ce qui a permis à la NSA d'avoir accès aux données détenues par des FST sans qu'un juge ait à approuver les requêtes[24].

25. Au Canada, cette façon de faire ne serait pas légale :

> « De façon générale, l'exercice des pouvoirs d'accès est assujetti à l'obtention d'une autorisation et nécessite une preuve par affidavit de motifs raisonnables indicatifs de la commission, ou d'un risque de commission d'une infraction, une description des démarches d'enquête effectuées et la portée de l'interception ou de la perquisition pour laquelle une autorisation est recherchée[25]. »

26. De plus, la Cour suprême a rejeté la doctrine de la tierce partie de façon constante depuis les années 90, car il y a une claire distinction entre le risque qu'un individu ait accès à certaines informations personnelles et le risque encouru en donnant à l'État l'autorisation de mettre la main sur des données personnelles sans qu'un mandat soit nécessaire[26]. La Cour suprême a en effet confirmé à plusieurs reprises le lien important qui unissait la vie privée et la démocratie : « … la vie privée constitue « une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère[27]. » »

27. Bref, ajouter au projet de décret à l'étude une instruction au CRTC visant la sécurité des infrastructures de télécom donnerait une assurance de plus aux Canadiennes et Canadiens que la protection de leurs renseignements personnels sera appuyée sur des bases solides. Avec les bouleversements technologiques prévisibles dans les prochaines années (opérations à distance, voitures autonomes, reconnaissance faciale, etc.), la quantité de données en circulation explosera et il n'est pas encore possible de savoir avec certitude qui détiendra ces données. La virtualisation des réseaux et des serveurs, par exemple, pourrait-elle faire en sorte que des informations sur les déplacements des

---

[20] Heidi Bohaker, Lisa Austin, Andrew Clement and Stephanie Perrin, *Seeing Through the Cloud – National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digital Interconnected World,* University of Toronto, 2015, p. 2.
[21] *Ibidem*, p. 6.
[22] Third party doctrine.
[23] Lisa M. Austin and Daniel Carens-Nedelsky, *Why Jurisdiction Still Matters*, University of Toronto, 31 mai 2015, p. 8.
[24] *Op. cit*., note 20, p. 8.
[25] Jean-François De Rico, *Chronique – L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements*, Repères, février 2014, p. 7.
[26] *Op. cit*, note 23, p. 8 à 10.
[27] R. c. Fearon, 2014 CSC 77, [2014] 3 R.C.S. 621, par. 116.

citoyennes et citoyens canadiens soient conservées par des entreprises américaines détenant des ententes d'interconnexion avec les FST canadiens?

28. En cette matière, le CPSC croit qu'il vaut mieux être prudent et que le gouvernement aurait intérêt à donner une instruction d'application générale claire au CRTC en matière de sécurité, laquelle aurait également des impacts sur le renforcement de la structure économique et sociale du pays, ainsi que sur la protection de la vie privée.

29. La population du Canada mérite que la sécurité des réseaux de télécommunication canadiens soit au premier rang des priorités du gouvernement et du CRTC, puisque le développement d'une économie numérique prospère et innovante dépend de cette sécurité et de la confiance qu'elle génère.

Espérant que ces quelques arguments auront apporté un éclairage pertinent au gouvernement en vue de l'adoption de son décret, nous vous prions d'agréer, Madame, nos salutations cordiales.

Nick Mingione
Président, CPSC