CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

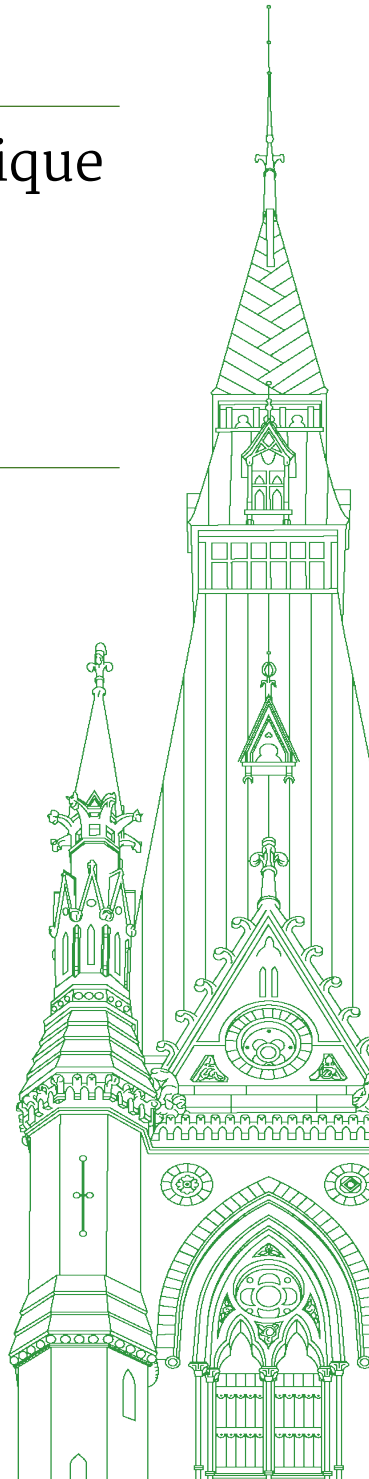
45e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 037

Le jeudi 7 mai 2026



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le jeudi 7 mai 2026

● (1535)

[*Traduction*]

Le vice-président (Frank Caputo (Kamloops—Thompson—Nicola, PCC)): La séance est ouverte.

Tout d'abord, je tiens à mentionner qu'en ma qualité de vice-président du Comité, je suis ravi et honoré de présider la réunion d'aujourd'hui. Merci beaucoup à toutes et à tous.

Bienvenue à la 37e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes. Conformément à l'ordre de renvoi de la Chambre du 20 avril 2026 et à la motion adoptée par le Comité le 30 avril 2026, le Comité reprend son étude du projet de loi C-22, Loi concernant l'accès légal.

Je souhaite la bienvenue aux témoins.

Nous recevons la professeure Leah West, à titre personnel; le chef Fleury, du Service de police de Thunder Bay; et le chef Demkiw, du Service de police de Toronto.

Bienvenue à vous.

Chaque témoin dispose de cinq minutes pour faire une déclaration préliminaire. Pour les personnes dans la salle, je vais tenter d'attirer votre attention lorsqu'il vous restera une minute, puis quand votre temps tirera à sa fin. J'espère pouvoir faire de même pour les personnes qui participent par vidéoconférence.

Sur ce, j'invite Mme West à faire sa déclaration préliminaire.

Merci.

Leah West (professeure agrégée, Norman Paterson School of International Affairs, Carleton University, à titre personnel): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invitée à témoigner aujourd'hui.

Si mon compte est bon, le projet de loi C-22 représente la neuvième tentative du Canada d'adopter une mesure législative sur l'accès légal. Il y a là matière à réflexion. Depuis plus de 10 ans, les gouvernements successifs ont reconnu l'existence du même problème: nous n'avons pas su adapter nos lois aux réalités des menaces actuelles en matière de criminalité et de sécurité nationale ni nous doter des outils législatifs nécessaires pour y faire face. Le résultat est un écart grandissant entre le cadre régissant l'accès légal au Canada et le rôle central que jouent les données électroniques dans les enquêtes et les poursuites pénales.

En même temps, la Cour suprême du Canada a indiqué clairement que même les identifiants de base sont susceptibles de révéler des renseignements extrêmement personnels et qu'ils sont donc protégés par l'article 8 de la Charte. Comme le tribunal l'a réaffirmé récemment, une adresse IP est souvent le premier fragment numérique lançant l'État sur la trace de l'activité en ligne d'un individu.

Le gouvernement et votre comité ont la lourde tâche de combler les lacunes opérationnelles existantes d'une manière qui soit conforme à la Charte. Le projet de loi C-22 représente une amélioration importante par rapport aux efforts de réforme déployés dans le passé. Il témoigne du travail acharné accompli par les gens de Sécurité publique Canada pour nouer le dialogue avec les parties prenantes et pour réviser les propositions antérieures. Il est mieux structuré et, selon moi, plus susceptible de mener à la mise en place d'un régime d'accès légal applicable. Toutefois, le travail n'est pas terminé.

Permettez-moi d'attirer votre attention sur trois éléments par rapport auxquels des amendements ciblés renforceraient considérablement le projet de loi.

Le premier concerne les ordonnances de communication de renseignements relatifs à l'abonné. Le projet de loi introduit un nouvel outil qui permet à la police d'obtenir les renseignements relatifs à l'abonné selon une norme de soupçon raisonnable. À mon avis, cette norme est constitutionnellement défendable, mais dans sa version actuelle, le projet de loi va trop loin à un autre égard. Il oblige les fournisseurs de services à communiquer tous les renseignements relatifs à l'abonné, tels que définis, associés à un identifiant, que chaque catégorie de données soit pertinente ou non pour l'enquête.

Ce nouveau pouvoir s'applique non seulement aux fournisseurs de services téléphoniques, mais aussi à quiconque fournit des services, ce qui risque d'entraîner une collecte excessive de renseignements personnels ne répondant pas aux critères énoncés dans le projet de loi. La solution est simple: il suffit de modifier la disposition afin de donner à la police le pouvoir discrétionnaire de demander uniquement des types précis de renseignements relatifs à l'abonné répondant à la norme, et aux juges le pouvoir discrétionnaire d'autoriser uniquement la communication de ce type de renseignements. Si la norme pour une ordonnance de communication est le soupçon, alors les éléments visés doivent être strictement définis.

Le deuxième élément se rapporte aux risques courus par les personnes à l'étranger. Le projet de loi permet aux autorités canadiennes de demander des renseignements directement aux fournisseurs de services situés à l'étranger. Ce pouvoir est important, mais il comporte des risques. À l'heure actuelle, le juge n'est pas tenu d'examiner si une telle demande pourrait exposer la personne visée à de mauvais traitements dans un autre pays. C'est une lacune. Je recommande d'imposer clairement aux juges l'obligation d'évaluer s'il existe un risque sérieux de mauvais traitements et de refuser la demande le cas échéant. Cette obligation harmoniserait le régime avec les engagements globaux du Canada en matière de droits de la personne et les exigences déjà imposées aux agents de la GRC en vertu de la Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères.

Le troisième élément et le plus important, c'est la partie 2, ou la Loi sur le soutien en matière d'accès autorisé à de l'information. Le fait d'obliger les entreprises à se doter de capacités d'interception et à conserver des données qu'elles ne garderaient pas autrement entraîne inévitablement des risques au chapitre de la cybersécurité. Chaque point d'accès supplémentaire et chaque nouvelle base de données constituent des cibles potentielles. La question n'est pas de savoir si le projet de loi crée de nouveaux risques; la réponse est oui. La question est de savoir s'il atténue suffisamment ces risques, et s'il établit un juste équilibre entre les risques et les impératifs de la sécurité publique. Sous sa forme actuelle, je pense que la réponse est non.

Trois modifications s'imposent.

Premièrement, il faut renforcer la définition du terme « vulnérabilité systémique » et interdire au gouverneur en conseil d'affaiblir cette définition par voie de règlement.

Deuxièmement, il faut interdire la conservation généralisée des données. À mon avis, les dispositions actuelles portent atteinte au droit à la vie privée, elles sont trop générales et elles créent un risque important en matière de cybersécurité. Le cadre actuel d'un an diffère considérablement des délais de conservation existants de 90 jours. Par ailleurs, je n'ai toujours pas entendu d'argument convaincant justifiant la nécessité d'une obligation de conservation généralisée des données qui ne soit pas liée à un pouvoir particulier de collecte ou à une catégorie précise d'infractions, comme les crimes graves. Tout régime de conservation des données doit être nécessaire à des fins d'enquête, et il doit être raisonnable et proportionnel à l'infraction ou à la menace faisant l'objet de l'enquête.

Troisièmement, il faut interdire explicitement aux organismes d'application de la loi et au SCRS de recueillir ou d'intercepter directement des renseignements personnels ou des données privées dans les systèmes des fournisseurs de services. Le contrôle de l'accès aux données et aux systèmes des fournisseurs doit rester entre les mains des fournisseurs. Eux seuls doivent détenir le pouvoir. C'est essentiel pour la protection de la vie privée, la sécurité et la clarté juridique.

● (1540)

En conclusion, je suis convaincue qu'une réforme de l'accès légal s'impose au Canada, mais il ne suffit pas d'élargir l'accès. Il faut également veiller à ce que tout nouveau pouvoir soit nécessaire, raisonnable et proportionnel; à ce qu'il n'affaiblisse pas les protections constitutionnelles; et à ce qu'il ne compromette pas indûment la sécurité de la population canadienne.

Le projet de loi C-22 représente une nette amélioration, mais pour faire mouche, il faut y apporter des amendements ciblés.

Merci.

Le vice-président (Frank Caputo): Merci, madame West. Vous avez terminé juste à temps.

Nous passons maintenant au chef Fleury, qui dispose de cinq minutes.

Le chef Darcy Fleury (chef de police, Service de police de Thunder Bay): Je vous remercie, monsieur le président, mesdames et messieurs les membres du Comité, de m'avoir invité à discuter avec vous aujourd'hui du projet de loi C-22, Loi concernant l'accès légal, et des raisons pour lesquelles les chefs de police aux quatre coins du Canada appuient fortement son adoption.

Au cours des 10 dernières années, les services de police au Canada ont connu une transformation radicale. Désormais, la criminalité dépasse les limites des espaces physiques et les frontières géographiques. Aujourd'hui, les réseaux du crime organisé opèrent au-delà des frontières en utilisant des applications chiffrées, des comptes anonymes et des plateformes numériques pour coordonner des activités telles que le trafic de stupéfiants, la traite de personnes, la contrebande d'armes et la cybercriminalité. Or, les lois qui régissent l'accès de la police aux renseignements essentiels ont été élaborées en grande partie avant l'avènement de l'ère numérique.

Le projet de loi C-22 vise à combler l'écart. Il propose des modifications pratiques et mesurées qui permettront aux enquêteurs d'accéder plus efficacement à certains renseignements, toujours avec autorisation légitime, sous contrôle judiciaire, et en respectant pleinement la Charte et les garanties en matière de protection de la vie privée auxquelles s'attend la population canadienne.

Il ne s'agit pas de conférer à la police des pouvoirs illimités; il s'agit de faire en sorte que lorsqu'elle a une raison légitime d'agir...

Le vice-président (Frank Caputo): Excusez-moi, chef Fleury. Puis-je vous interrompre un instant? Pouvez-vous baisser légèrement votre microphone pour qu'il ne touche pas votre peau?

Le chef Darcy Fleury: D'accord.

Est-ce que c'est mieux?

Le vice-président (Frank Caputo): On me fait signe que oui.

Merci. Désolé de vous avoir interrompu.

Le chef Darcy Fleury: Je vous en prie. Merci.

Il ne s'agit pas de conférer à la police des pouvoirs illimités; il s'agit de faire en sorte que lorsqu'elle a une raison légitime d'agir, elle puisse le faire rapidement, surtout quand des vies sont menacées.

Nous sommes des experts en la matière. L'an dernier seulement, le Service de police de Thunder Bay a enquêté sur 184 dossiers liés à la cybercriminalité, ce qui représentait plus de 140 ordonnances de communication, 80 mandats de perquisition et au-delà de 1 370 appareils saisis à des fins d'examen. Ces efforts nous ont permis d'identifier 20 victimes et de porter plus de 240 accusations. C'est impressionnant pour une unité de cinq personnes.

Cela dit, ce n'est pas une question de statistiques; c'est une question de protéger les gens. Le projet de loi C-22 aidera les services de police comme le nôtre, qui disposent de ressources limitées pour répondre à une demande croissante, à intervenir plus rapidement auprès des victimes. Permettez-moi de vous donner un exemple concret.

Imaginez qu'une jeune fille de 14 ans est portée disparue. Elle s'appelle Shawna. Selon ses parents, elle communiquait en ligne avec une personne qui l'exploitait. Les enquêteurs trouvent un nom d'utilisateur associé à une plateforme de messagerie. Le temps presse. Dans le cadre actuel, il faut plusieurs heures précieuses, voire des jours, pour confirmer quel fournisseur de services détient les renseignements liés au compte et pour obtenir les données de base de l'abonné qu'il faut pour agir, étant donné la fragmentation des processus et l'obsolescence des voies légales.

Entretemps, des preuves montrent que le suspect pourrait tenter de déplacer Shawna vers une autre province ou un autre pays. Chaque minute compte. En vertu du projet de loi C-22, il faudra moins de temps pour que les enquêteurs confirment quel fournisseur de services est associé au compte et pour qu'ils obtiennent l'autorisation judiciaire requise pour recueillir de nouveaux éléments de preuve. En cas d'urgence, ils pourront demander un accès limité aux données afin de prévenir un préjudice imminent, tout en demeurant pleinement soumis à des critères juridiques stricts et à un contrôle rigoureux. Grâce au temps ainsi gagné, on pourrait trouver Shawna avant qu'elle soit déplacée, avant que plus de mal soit fait et avant que des éléments de preuve essentiels disparaissent.

C'est une réalité à laquelle les services de police font face au quotidien. À Thunder Bay, de nombreuses victimes d'exploitation, dont des jeunes d'à peine 14 ans, nous parviennent du sud de l'Ontario. L'Association canadienne des chefs de police appuie le projet de loi C-22 parce qu'il établit un juste équilibre. Il simplifie l'accès aux renseignements essentiels, il améliore la communication de données en cas d'urgence et il clarifie la fourniture volontaire, tout en maintenant des garanties judiciaires et des mesures de protection de la vie privée rigoureuses. L'Association des chefs de police de l'Ontario réclame aussi depuis longtemps la modernisation des outils d'accès légal.

Nos membres voient bien comment les individus et les réseaux du crime organisé exploitent les lacunes législatives. Ces acteurs sont sophistiqués et ils évoluent constamment.

Pour assurer la sécurité des collectivités, les services de police doivent aussi évoluer. Les outils d'accès légal ne visent pas à accroître indûment la surveillance; ils visent à protéger le public. Ils permettent aux enquêteurs de comprendre les réseaux criminels, de prévenir la violence et de secourir les victimes. Qu'on cherche à trouver une jeune fille portée disparue, à perturber le trafic de fentanyl, à démanteler un réseau de traite de personnes ou à combattre l'exploitation en ligne, il faut absolument des cadres juridiques clairs et des outils modernes.

Le projet de loi C-22 représente un pas important dans la bonne direction. Il reconnaît que les crimes modernes exigent des solutions modernes. Il permet à la police d'agir rapidement dans les situations d'urgence, tout en respectant strictement les autorisations judiciaires, la législation sur la protection de la vie privée et la Charte des droits et libertés. Fondamentalement, le projet de loi vise à protéger les Canadiennes et les Canadiens, en particulier les plus vulnérables d'entre nous.

Je vous exhorte à appuyer l'adoption rapide du projet de loi C-22.

Merci.

● (1545)

Le vice-président (Frank Caputo): Merci, chef Fleury.

Nous passons maintenant au chef Demkiw. Vous disposez de cinq minutes.

Chef Myron Demkiw (chef de police, Toronto Police Service): Je remercie les membres du Comité permanent de la sécurité publique et nationale de m'avoir invité à être ici aujourd'hui.

Le Service de police de Toronto, de pair avec l'ensemble des forces policières du Canada, milite depuis longtemps en faveur de réformes donnant la priorité à la sécurité publique, y compris des réformes visant l'accès légal. Nous sommes d'avis que le projet de loi C-22, Loi concernant l'accès légal, est un pas dans la bonne direction. Il fournira aux agents des outils supplémentaires qui leur permettront de faire avancer plus rapidement les enquêtes, de tenir les délinquants responsables de leurs actes et de prévenir les préjudices.

La prévention des préjudices requiert souvent une intervention rapide, y compris dans les cas d'extrémisme violent.

Le Service de police de Toronto est le plus grand service de police municipal au Canada. Il est extrêmement complexe d'assurer le maintien de l'ordre à Toronto. Outre tous les aspects uniques de la ville, on y observe souvent des tendances avant qu'elles ne se manifestent ailleurs. Les répercussions des réalités géopolitiques s'y font sentir, et les crimes haineux y sont à la hausse. De plus, des situations survenant sur le terrain sont ancrées dans la complexité des enjeux de santé mentale, de toxicomanie et de besoins sociaux non satisfaits.

En outre, la majorité des bureaux consulaires de l'Ontario sont situés à Toronto. Aussi, la ville accueille de nombreux grands événements internationaux. Par ailleurs, on constate qu'un nombre croissant de jeunes se livrent à des actes de violence; souvent, ces jeunes se servent de plateformes numériques pour communiquer de manière anonyme au sujet de cibles potentielles.

Pour résoudre ces problèmes, il faut le soutien et la collaboration de l'ensemble du système de justice, y compris pour réformer la législation. À de nombreux égards, les nouvelles technologies et l'amélioration des communications ont simplifié nos vies, mais grâce à elles, il est aussi plus facile pour les criminels de planifier leurs activités et d'échapper à la justice. Des acteurs malveillants utilisent des outils numériques pour commettre des crimes de toutes les catégories, y compris le trafic de stupéfiants, l'extorsion, la pornographie juvénile, les crimes haineux, l'extrémisme et d'autres infractions graves.

Notre rôle consiste à prévenir ces infractions, à faire traduire les délinquants en justice et à donner une voix aux victimes qui ont connu des situations des plus difficiles. Toutefois, puisque la technologie a évolué si rapidement ces dernières années, les enquêteurs rencontrent parfois des obstacles.

Prenez, par exemple, la question de confirmer quel fournisseur de services de télécommunication détient les renseignements qui serviront à une enquête. À l'heure actuelle, ce processus prend beaucoup de temps et il peut entraîner la perte d'éléments de preuve. Le projet de loi C-22 simplifiera les processus et il permettra à la police de faire avancer les enquêtes en temps opportun.

Les organismes d'application de la loi et le système de justice doivent évoluer au même rythme que la criminalité. Il est important de souligner que d'autres pays du Groupe des cinq utilisent déjà certains des outils proposés. Le Service de police de Toronto est convaincu que le régime d'accès légal accélérera l'accès aux renseignements essentiels, et par le fait même, qu'il renforcera la sécurité publique.

Merci. Nous sommes impatients de poursuivre notre collaboration avec tous les ordres de gouvernement pour faire en sorte que le système de justice assure la responsabilité et protège nos collectivités.

● (1550)

Le vice-président (Frank Caputo): Merci, monsieur Demkiw.

Sur ce, nous allons passer à notre première série de questions. Je vais exercer ma prérogative de président et prendre six minutes pour poser des questions. J'en ai discuté avec l'honorable secrétaire parlementaire et mon collègue du Bloc.

Merci à tous de votre présence. C'est un domaine dans lequel vous avez tous beaucoup d'expertise.

Je remercie les deux chefs de police de leur service.

Madame West, vous ne serez probablement pas étonnée que je commence par vous. Je voulais vous poser une question sur le chiffrement, qui semble être un important problème pour certaines personnes.

Que pouvez-vous dire sur la notion de « chiffrement » qui se trouve dans le projet de loi? Est-elle assez bien définie, ou non? Qu'en pensez-vous, d'un point de vue juridique, étant donné ce que l'on trouve dans le projet de loi par rapport à la définition de « chiffrement »?

Leah West: Selon mon interprétation du projet de loi, le gouvernement n'a aucun moyen de vous obliger à déchiffrer vos données si vous n'avez pas déjà les capacités nécessaires.

Je dis cela parce que, tant pour les règlements que pour les arrêtés ministériels, il est précisé que vous n'êtes pas tenu de vous conformer à un décret ou à un règlement si le fait de s'y conformer oblige à introduire une « vulnérabilité systémique » dans votre système, et cette vulnérabilité systémique comprend le chiffrement, selon la définition actuelle de « protection électronique ».

Ce qui me préoccupe davantage, c'est la possibilité que d'autres formes de vulnérabilités systémiques intégrées au matériel ou au système d'exploitation ne soient pas comprises dans la définition de « vulnérabilité systémique ». Voilà où il y a une lacune, à mon avis.

Le vice-président (Frank Caputo): D'accord. Je me dois de vous demander de nous en dire plus à ce sujet, s'il vous plaît.

Lorsque vous parlez de ces vulnérabilités, je suppose qu'il peut s'agir de vulnérabilités dont le fournisseur n'a même pas connaissance. Est-ce exact?

Leah West: C'est exact. Cependant, puisque nous ignorons qui seraient les fournisseurs principaux ni qui pourrait être visé par cette loi, il est possible que certains fournisseurs de matériel, par exemple, soient des fournisseurs de services visés, et la définition de « vulnérabilité systémique », dans sa forme actuelle, n'inclurait pas leurs activités.

Je sais que vous entendrez le professeur Diab, plus tard. Il a également réfléchi à cette question, alors à votre place, je lui demanderais d'en dire plus à ce sujet.

Le vice-président (Frank Caputo): C'est vrai, car la partie 2 du projet de loi s'appliquerait aux fournisseurs correspondant à la définition de « fournisseur principal » ou, si je me souviens bien, à ceux qui sont désignés par arrêté ministériel. Est-ce que...

Leah West: C'est ce que je comprends, oui.

Le vice-président (Frank Caputo): Théoriquement, une entreprise pourrait être désignée par arrêté ministériel, et elle serait alors assujettie à cette disposition. Essentiellement, si je comprends bien ce que vous dites, il n'y a pas de limite, dans la mesure où nous ne savons pas exactement à qui cela s'appliquera. Ai-je bien compris?

Leah West: D'après ce que je comprends, il faudrait quand même que ce soit un fournisseur de services électroniques. Cependant, la définition de « fournisseur de services électroniques » est plutôt large, de sorte qu'elle pourrait englober les personnes qui fournissent des services de matériel, par exemple.

Le vice-président (Frank Caputo): J'ai une question au sujet d'un aspect intéressant qui a été porté à mon attention. Disons qu'un fournisseur a la capacité... Je parle d'Alexa, par exemple. C'est Amazon, je pense. Est-ce bien cela? C'est quelque chose comme ça. En théorie, Alexa pourrait écouter vos conversations, ou chaque fois que vous dites « Hé, Siri », Siri commence à écouter.

Si Apple — je suis désolé de cibler Apple — ou toute autre entreprise a cette capacité, pourrait-elle dire que chaque fois qu'une personne dit « Hé, Siri », cette application doit commencer à écouter?

L'application elle-même ou le fournisseur lui-même a la capacité d'écouter. Il ne s'agit pas nécessairement de demander au fournisseur de créer un nouveau pouvoir. Cela revient presque à lui demander d'aller un peu plus loin.

Me suivez-vous jusqu'ici?

Leah West: Oui.

Le vice-président (Frank Caputo): D'après ce que je comprends, si un tel arrêté ministériel était pris, cet arrêté ne serait pas « possiblement » secret, mais serait secret, de sorte qu'un dénonciateur ne pourrait pas nécessairement se manifester. Je suppose que le seul recours de l'entreprise qui le ferait serait de demander un contrôle judiciaire. Est-ce exact?

● (1555)

Leah West: Tout arrêté ministériel visant à accorder ce pouvoir devrait faire l'objet d'un examen et être approuvé par le commissaire au renseignement, et alors, oui... mais avec des consultations. Il existe une exigence pour la tenue de consultations, avec Apple dans ce cas-ci. Si cette approbation était toujours accordée, il y aurait un recours judiciaire.

Cependant, à cela s'ajoute le fait que personne ne pourrait accéder à cela légalement sans mandat d'interception. Le simple fait que le fournisseur de services en ait la capacité ne signifie pas nécessairement que les organismes d'application de la loi y auraient soudainement accès. Dans ce cas, on ne créerait pas vraiment une nouvelle vulnérabilité, car ils avaient déjà cette capacité. Essentiellement, on ne fait que donner aux organismes d'application de la loi la capacité de tirer parti d'un instrument qui existait déjà, s'ils avaient l'autorité légale.

Le vice-président (Frank Caputo): D'accord. Je suppose que, dans ce cas, la différence pourrait être que la police pourrait dire: « Nous pensons que Mme West a commis une infraction criminelle, et que son utilisation de Siri le prouve. Nous allons obtenir un mandat. » Ils ont déjà cette possibilité maintenant. La seule différence, c'est qu'en vertu de la partie 2, il faudrait invoquer la capacité ou les moyens de le faire, alors qu'actuellement, cela n'existerait tout simplement pas, si cela a du sens.

Leah West: C'est ce que je comprends.

Le vice-président (Frank Caputo): D'accord. Merci.

Mes six minutes sont écoulées.

[*Français*]

Monsieur Ramsay, vous avez la parole pour six minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Merci.

Ma question s'adressera aux deux représentants des forces de l'ordre. L'une des choses importantes à mettre en perspective, ici, c'est que le projet de loi C-22 vise à donner aux forces de l'ordre les moyens d'agir en temps opportun.

Chef Demkiw, vous avez dit que le processus était chronophage, que ça pouvait causer une perte d'éléments de preuve.

Par ailleurs, selon vous, dans les cas de fraudes sur Internet, de cybercriminalité, d'extorsion, de vols de véhicules, ai-je raison de penser que le fait d'agir rapidement permet de réduire le nombre de victimes?

Si une enquête dure un an ou 18 mois, il peut y avoir des centaines de victimes, au lieu de quelques cas ou quelques dizaines de cas. S'il s'agit de cybercriminalité ou de sextorsion, il peut y avoir de nombreuses victimes.

C'est là-dessus que je voudrais avoir une clarification. Il y a une grande différence entre avoir une victime ou en avoir 200, entre avoir un cas de cybercriminalité ou en avoir 12.

C'est là-dessus que le projet de loi C-22 doit changer les choses.

Quelles sont vos observations à ce sujet?

[*Traduction*]

Chef Myron Demkiw: La réponse courte est oui, il est important d'agir en temps opportun, et lorsque le temps est un facteur crucial, qu'il s'agisse de cybercriminalité, de fraude ou d'extorsion, le risque de victimisation s'accroît inévitablement. Je parle tant du nombre de victimes que des répercussions sur chacune des victimes. Comme nous le savons, il arrive que des personnes soient victimes à plusieurs reprises.

Pour répondre à votre question, puisque nos enquêtes sont parfois entravées et qu'il faut plus de temps pour trouver les preuves numériques nécessaires pour mettre fin à la victimisation et à la criminalité, plus de personnes sont victimes.

Jacques Ramsay: Chef Fleury, voulez-vous ajouter quelque chose?

Le chef Darcy Fleury: Oui.

Étant donné l'exemple des infractions de fraude que vous avez utilisé, prenons l'exemple d'une pyramide de Ponzi. Dans un tel cas, si nous avons identifié une, deux ou trois victimes et que nous avons la possibilité d'accéder rapidement au matériel ou aux renseignements, il est alors fort probable que cet accès rapide nous permette d'empêcher que d'autres personnes ne soient victimes avant même que nous terminions l'enquête.

J'ai déjà vu cela se produire dans le passé, lorsqu'il était urgent d'agir. On parle d'individus très motivés à commettre leur crime qui peuvent faire plusieurs victimes très rapidement. Si nous avons la possibilité d'intervenir, nous pourrions mettre fin à leurs activités tandis que nous établissons les motifs pour porter des accusations et les traduire en justice. Je pense qu'il est primordial, dans de telles circonstances, d'avoir un accès rapide.

● (1600)

[*Français*]

Jacques Ramsay: Merci.

Nous avons parfois l'impression que certaines personnes voudraient faire paraître le projet de loi C-22 comme étant excessif. Au contraire, je pense que, par ce projet de loi, le gouvernement a fait preuve de beaucoup de tempérance et qu'il a insisté simplement sur ce qui était essentiel. À un moment, on a pensé demander des informations sur les véhicules de taxi, sur ce qui se passe la nuit dans les hôtels. Le gouvernement a décidé de restreindre ces pouvoirs.

Selon vous, le projet de loi C-22 représente-t-il une pièce législative posée, qui ne va chercher que les informations essentielles?

[*Traduction*]

Chef Myron Demkiw: Si vous me permettez de commencer, la réponse courte est oui, je pense que c'est le cas.

Nous savons par expérience que l'utilisation des technologies numériques par les criminels s'est considérablement accrue, et notre capacité de collecter et de préserver des éléments de preuve en temps opportun et de prévenir l'escalade des infractions est entravée par l'incapacité d'accéder à d'importants éléments de preuve numériques. Le projet de loi C-22 nous sera utile à cet égard.

Voici un exemple simple. Lorsqu'un numéro de téléphone est lié à un ensemble d'actes criminels, quelle que soit la gravité des crimes allégués, nous devons déterminer quel est le fournisseur de services, ce qui est, en soi, une tâche fastidieuse de nos jours. Le projet de loi C-22 simplifiera cette tâche, ce qui nous permettra d'agir plus rapidement et de collecter des preuves essentielles qui, dans le cadre législatif actuel, pourraient disparaître et être perdues tandis que nous attendons des informations de divers fournisseurs de services pour faire avancer nos enquêtes.

Le projet de loi C-22 est bien conçu pour nous aider à accéder plus facilement et en temps opportun aux technologies numériques essentielles.

Le chef Darcy Fleury: Oui, je suis d'accord avec le chef Demkiw. Je pense que le projet de loi est très bien conçu et couvre les domaines où les données circulent très rapidement. Il est fort utile pour la collecte de données.

Jacques Ramsay: Madame West, je crois savoir que le Canada et l'Australie sont les seuls pays où il est explicitement interdit, en matière de mesures de protection électronique, de mettre en place un dispositif susceptible d'introduire une vulnérabilité systémique. Par exemple, aux États-Unis...

[*Français*]

Le vice-président (Frank Caputo): Je suis désolé, monsieur Ramsay. Votre temps de parole est écoulé.

[*Traduction*]

Non, je n'avais pas hâte de le dire.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Merci beaucoup, monsieur le président.

Professeure West, dans une lettre conjointe, plusieurs organisations de la société civile ont exprimé des inquiétudes à propos du projet de loi C-22. On dit qu'il pourrait faciliter l'accroissement des échanges d'information avec des gouvernements étrangers, y compris des États dont les pratiques en matière de droits de la personne sont préoccupantes.

Quelles protections supplémentaires devraient être envisagées pour limiter l'utilisation ultérieure des renseignements personnels concernant des Canadiens?

[*Traduction*]

Leah West: Je pense qu'il y a deux problèmes.

Le premier est lié aux modifications au Traité d'entraide juridique, qui permettraient à des entités étrangères de signifier des ordonnances au Canada. Il y aurait un processus dans le cadre duquel le ministre approuverait la demande, qui serait ensuite renvoyée à un juge qui serait chargé de déterminer que la demande satisfait aux critères énoncés dans le Code criminel, puis les données pourraient être collectées.

Rien n'exige que l'infraction faisant l'objet d'une enquête soit également une infraction au Canada. Il est donc possible que des gouvernements étrangers cherchent à faire appliquer des lois répressives ou à mener des enquêtes pour des motifs politiques dans le cadre de ce processus. Il n'existe pas de véritable mesure pour empêcher cela, si ce n'est que le ministre peut agir à sa discrétion. Dans ce cas, en particulier parce qu'un juge ne participe pas nécessairement au processus dans le pays étranger, il peut s'agir d'une ordonnance administrative. Le ministre doit s'engager à exercer son pouvoir discrétionnaire et ne pas donner son autorisation lorsqu'une enquête relative à une infraction est susceptible d'être menée à des fins répressives ou politiques. La mesure législative ne prévoit aucune mesure de protection.

Ce serait possible grâce à l'ajout d'une disposition précisant que l'infraction doit également être considérée comme un acte criminel au Canada. Cela éliminerait ce problème. C'est une façon d'élargir la portée. Actuellement, cependant, ce serait à la discrétion du ministre.

● (1605)

[*Français*]

Claude DeBellefeuille: Merci.

Cette question me préoccupe beaucoup. Alors, si vous pouviez nous suggérer un amendement précis à apporter au projet de loi C-22 qui pourrait rassurer les gens, ce serait très utile. Nous avons jusqu'au 27 mai pour déposer des amendements.

J'aimerais vous poser une autre question. Dans la lettre que vous avez publiée dans le *Globe and Mail*, vous soulignez l'importance du travail qui se fait en comité et d'un consensus autour du projet de loi C-22. Je pense que tout le monde ici est prêt à dire que ce projet de loi est nécessaire, mais qu'il pourrait être bonifié.

Selon vous, serait-il raisonnable d'y inclure l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, pour que celui-ci soit notifié en temps réel lorsqu'un arrêté ministériel est pris, ainsi que pour qu'il puisse faire enquête et veiller à ce qu'on n'abuse pas des pouvoirs qui seraient conférés par le projet de loi C-22?

[*Traduction*]

Leah West: Non, je ne pense pas. L'Office de surveillance des activités en matière de sécurité nationale et de renseignement est un organisme d'examen. Il procède à un examen *ex post facto*. Actuellement, il n'a pas un mandat de surveillance.

J'ai personnellement recommandé que le commissaire au renseignement participe à l'examen des arrêtés ministériels, parce qu'il exerce ce rôle de surveillance dans le système actuel et qu'il a la capacité nécessaire pour le faire, ce que l'OSSNR n'a pas.

[*Français*]

Claude DeBellefeuille: D'accord.

L'idée n'est pas que l'Office de surveillance des activités en matière de sécurité nationale et de renseignement prenne part à la décision ou donne son opinion sur la poursuite de l'arrêté ministériel. Il s'agit plutôt d'assurer que l'Office est notifié en temps réel pour qu'il soit capable de documenter un dossier qui, une fois l'année écoulée, pourrait être plus facile à traiter si jamais une enquête était déclenchée.

Je vous remercie de préciser votre opinion parce que, même avec l'aide de l'interprétation, c'est un peu difficile pour moi de comprendre.

[*Traduction*]

Leah West: À mon avis, l'OSSNR a certainement un rôle à jouer dans l'examen du système en général et vos collègues du CPSNR pourraient également y contribuer à l'avenir. Ce sera extrêmement important, notamment pour examiner la façon dont se dérouleront les échanges avec les fournisseurs de services.

Quant à savoir si l'OSSNR doit être informé chaque fois qu'un arrêté ministériel est pris à cette fin... Encore une fois, je pense qu'il est davantage conçu pour la fonction d'examen à plus long terme. Il serait préférable de recevoir l'information à la fin de l'année civile ou tous les six mois. À mon avis, il n'est pas vraiment en mesure de faire des examens au cas par cas.

[*Français*]

Claude DeBellefeuille: Vous avez dit que la définition du terme « fournisseur de services électroniques » est très large et qu'elle pourrait inclure, par exemple, des fournisseurs de matériel.

Pourriez-vous nous donner des exemples concernant les fournisseurs de matériel?

[*Traduction*]

Leah West: Habituellement, tous ceux qui fournissent du matériel offrent également des services électroniques quelconques. Je pense que les fournisseurs de matériel, notamment Ericsson et d'autres entreprises du secteur du matériel, pourraient être visés par la définition générale.

Je ne pense pas que ce soit nécessairement mauvais. Je pense que la définition...

Le vice-président (Frank Caputo): Je suis désolé, madame West. Nous devrons y revenir au prochain tour.

Nous passons à Mme Kirkland pour cinq minutes, s'il vous plaît.

Rhonda Kirkland (Oshawa, PCC): Merci.

Mes questions s'adressent à Mme West.

Je vous remercie de votre témoignage.

Puisque c'est la neuvième fois, comme vous l'avez dit, que nous essayons de faire les choses correctement en ce qui a trait à l'accès légal, dans quelle mesure est-il important — vous avez parlé de trouver le bon équilibre — de ne pas nous précipiter pour obtenir la sanction royale, mais plutôt de prendre le temps d'examiner les amendements et d'écouter les témoignages?

● (1610)

Leah West: Je pense que c'est essentiel pour adopter un bon projet de loi.

Rhonda Kirkland: Merci.

Vous avez dit publiquement que le gouvernement devrait montrer qu'il a fait ses devoirs. Je vous en remercie, en particulier à la lumière de l'attention accordée au Comité, qui joue un rôle pour aider le projet de loi à franchir les étapes du processus.

Nous savons qu'en consultation avec M. Murray Rankin, qui a produit un rapport qui a servi à l'élaboration du projet de loi C-22... Le ministre de la Sécurité publique a dit au Comité que le rapport avait spécifiquement servi à éclairer les décisions du gouvernement concernant le projet de loi C-22. Je sais que vous avez participé directement à ces consultations.

Selon votre avis professionnel, y a-t-il des motifs de sécurité nationale ou des motifs opérationnels légitimes qui font en sorte que le rapport est protégé par le secret professionnel et qui empêchent sa divulgation au Parlement ou à la population canadienne?

Leah West: Je ne suis pas au courant de la relation que M. Murray Rankin entretenait avec le ministre lorsqu'il l'a conseillé, donc non.

Rhonda Kirkland: De votre point de vue, en tant que participante au processus, dans quelle mesure l'exercice de consultation a-t-il joué un rôle déterminant pour élaborer les dispositions sur l'accès légal dont le Parlement est actuellement saisi?

Leah West: À mon avis, cela reflète le genre de conseils que j'ai entendus dans le cadre du processus de consultation.

Rhonda Kirkland: À votre connaissance, les participants au processus de consultation ont-ils été avisés que le rapport ou ses conclusions resteraient confidentiels et ne seraient pas divulgués au Parlement?

Leah West: Nous n'en avons pas discuté.

Rhonda Kirkland: Vous n'en avez jamais parlé. D'accord. Merci.

J'ai une dernière question.

Selon votre expérience, est-ce habituel? Vous avez probablement déjà participé à de tels processus. Je suppose que oui, mais je pourrais me tromper. Est-il habituel de garder entièrement secrets des rapports de consultation auxquels des experts et des intervenants externes ont participé? Avez-vous déjà vu cela?

Leah West: Je n'ai jamais participé à une consultation dirigée par une tierce partie, alors je ne suis pas certaine. Je participe généralement à des consultations menées par le gouvernement lui-même, et elles sont habituellement...

Le vice-président (Frank Caputo): Permettez-moi de vous interrompre brièvement, s'il vous plaît.

Nous sommes en pleine réunion. Les chuchotements ne me dérangent pas, car je sais que c'est inévitable, mais si certains doivent tenir une réunion, veuillez le faire à l'extérieur, s'il vous plaît. Merci.

Je suis désolé.

Leah West: Pas de souci.

Je n'ai jamais participé à un processus comme celui-ci. Dans le passé, dans le cadre de consultations gouvernementales, j'ai vu des rapports de type « Ce que nous avons entendu » qui ont été publiés. Il s'agissait de processus différents.

Rhonda Kirkland: Il semble possible que vous ayez vu le rapport dans le cadre du processus. Pouvez-vous nous dire si cela nous serait utile dans...

Leah West: Je n'ai pas vu le rapport.

Rhonda Kirkland: D'accord.

Leah West: J'ai vu une liste de recommandations.

Rhonda Kirkland: Vous avez vu une liste de recommandations.

Sans divulguer quelque information confidentielle que vous auriez vue, pouvez-vous dire au Comité si le rapport reflétait une diversité de points de vue? Savez-vous si, dans les recommandations, des experts et des intervenants ont soulevé des préoccupations et des mises en garde relativement à la protection des renseignements personnels?

Leah West: Oui, parce que mes propres préoccupations ont été prises en compte dans la liste de recommandations.

Rhonda Kirkland: Merci.

En parallèle de ce rapport, j'aimerais que vous nous en disiez plus sur les amendements que vous recommandez. Pourriez-vous en nommer un ou deux qui, selon vous, amélioreraient grandement le projet de loi? Nous savons à quel point l'accès légal est important. Je suis ravie que les chefs participent à la réunion d'aujourd'hui étant donné l'importance de l'enjeu.

Pouvez-vous nous donner un ou deux amendements qui pourraient sembler assez simples et sur lesquels nous pourrions tous nous entendre pour bien peaufiner le projet de loi plutôt que de nous précipiter...?

Leah West: Oui.

Comme je l'ai mentionné, j'implore le Comité d'écouter des experts techniques qui savent, plus qu'un avocat, comment englober tous les types de vulnérabilités que vous aimeriez éviter dans la définition de « vulnérabilité systémique. » Je trouve également que le libellé actuel de la disposition sur la conservation est trop large. Des dispositions semblables — même des dispositions plus étroitement adaptées en Europe — faisant intervenir le droit à la vie privée ont été jugées déraisonnables. Je pense que cette disposition doit être amendée pour veiller à ce que tout règlement soit étroitement ciblé, nécessaire, proportionnel et reflète le sérieux de ce qui est demandé, soit la création de grands bassins de données privées.

Rhonda Kirkland: Merci.

Nous savons que les définitions vagues amènent souvent les gouvernements futurs à utiliser les lois à mauvais escient ou à les détourner...

Le vice-président (Frank Caputo): Malheureusement, madame Kirkland, votre temps est écoulé.

La parole est maintenant à Mme Acan pour cinq minutes.

● (1615)

Sima Acan (Oakville-Ouest, Lib.): Merci beaucoup, monsieur le président.

Madame Leah, je suis ravie de vous revoir.

Ma question porte sur les demandes d'entités étrangères. Le Canada est actuellement le seul membre du Groupe des cinq et du G7 qui n'a pas de loi modernisée sur l'accès légal. L'absence d'un cadre de capacité technique nuit-elle à notre capacité de coopérer avec des partenaires internationaux sur les menaces transnationales? Comment le nouveau mécanisme prévu à la partie 1 pour les demandes d'entités étrangères résout-il ce problème?

Leah West: Oui, l'absence de cadre nuit à notre capacité de coopérer.

D'après mes discussions avec des intervenants des pays du Groupe des cinq, je crois comprendre que le seuil à partir duquel les autres pays peuvent obtenir des renseignements sur les abonnés est inférieur à celui du Canada. Dans les autres pays, il n'est souvent pas nécessaire d'obtenir une autorisation judiciaire, ou alors on peut s'appuyer sur des motifs raisonnables de soupçonner ou même sur une norme encore moins exigeante. Si les autres pays essaient d'utiliser le processus des traités d'entraide juridique au Canada, nous ne pouvons faire respecter leurs ordonnances puisqu'il n'y a pas d'équivalent au Canada.

En nous dotant d'une nouvelle disposition axée précisément sur les renseignements des abonnés et les données de transmission obtenus grâce aux motifs raisonnables de soupçonner, nous pourrons mieux collaborer avec les administrations étrangères. En effet, un tel régime s'harmoniserait mieux à leur mécanisme pour obtenir des renseignements sur les abonnés dans leur territoire et permettrait une application uniforme de la loi.

Sima Acan: Merci beaucoup.

Je me concentrerai principalement sur le volet opérationnel des services de police et sur les moyens de soutenir le travail des enquêteurs en ce qui concerne le crime organisé, l'extrémisme, l'exploitation sexuelle des enfants et d'autres crimes complexes.

Messieurs les chefs de police, le projet de loi C-22 crée une disposition pour confirmer la fourniture de services, qui simplifie le processus par lequel les forces de l'ordre identifient le fournisseur de services à qui adresser une ordonnance de communication. Diriez-vous que cette disposition est utile dans le contexte d'une enquête urgente sur le crime organisé, l'extrémisme, la haine ou l'exploitation d'enfants? Quels seront les principaux avantages opérationnels de cette disposition?

Chef Myron Demkiw: Merci de cette question.

Je pense que, dans les faits, nous avons souvent un numéro de téléphone ou un autre indice qui nous amène à vérifier l'empreinte ou les preuves numériques que le numéro de téléphone ou d'autres renseignements fournissent.

Dans le régime actuel, aucune disposition ne nous permet de demander qui est le fournisseur de services. Par exemple, nous devons émettre plusieurs ordonnances de communication simplement pour établir que le service est fourni par une entreprise de télécommunications en particulier. On y consacre énormément de temps. À titre d'exemple, sur une période de 20 mois, les activités de nos détectives à Toronto ont nécessité à elles seules 1 900 ordonnances de communication.

Ce qui nous aiderait beaucoup, ce serait d'avoir la capacité de comprendre sur quel fournisseur de services concentrer nos efforts d'enquête et de poursuivre ces enquêtes au moyen d'un processus visé par un examen judiciaire — c'est-à-dire grâce à des ordonnances de communication ou à des mandats. En gagnant ainsi du temps, nos chances de succès augmenteront véritablement.

Comme on l'a abordé dans la question précédente, les preuves qui peuvent être perdues — des enregistrements vidéo, des preuves médico-légales — pendant que nous déterminons qui est le fournisseur de services peuvent se traduire par une plus grande victimisation ou une victimisation qui se poursuit sur une plus longue période. Nous accueillons très favorablement la capacité de savoir rapidement où concentrer nos enquêtes, puis de recueillir des preuves au moyen d'ordonnances de communication examinées par un juge.

Sima Acan: Merci beaucoup.

Dans ce contexte, le projet de loi C-22 prévoit des exigences en matière de conservation des métadonnées selon lesquelles elles doivent être conservées pendant une période maximale de 12 mois. Hier, des fonctionnaires nous ont dit que, en Australie, les données sont conservées pendant deux ans, et pendant un an au Royaume-Uni.

Diriez-vous qu'il est raisonnable d'exiger que les fournisseurs principaux conservent les métadonnées pendant 12 mois, compte tenu de la rapidité avec laquelle ils les suppriment parfois? Il arrive que le délai soit de 30 jours ou de trois mois.

Le délai proposé offre de la souplesse aux fournisseurs et appuie le travail des enquêteurs, surtout étant donné que les cas complexes peuvent durer plus de trois à six mois, voire plus d'un an.

Le chef Darcy Fleury: Je pourrais répondre en premier, puis le chef pourra renchérir sur ma réponse.

Oui, je pense qu'un délai de 12 mois est un bon début, mais effectivement, vous avez évidemment raison. Lorsque les enquêtes se prolongent — et elles peuvent être très longues dans certains cas —, il serait idéal de conserver les données pendant plus de 12 mois — de 24 à 36 mois.

● (1620)

Le vice-président (Frank Caputo): Je suis désolé, chef Fleury. Je dois vous interrompre.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour deux minutes et demie.

Claude DeBellefeuille: Merci, monsieur le président.

Madame West, vous avez entendu les deux policiers discuter de la durée de conservation des données. Vous nous avez dit qu'un an, c'est trop. Les gens qui travaillent pour les services policiers viennent de nous dire que, pour eux, un an, c'est le minimum, et que deux ou trois ans, ce serait encore mieux.

Comment voyez-vous les choses?

Est-ce que vous tendez davantage vers une période de conservation plus courte? Comment réagissez-vous à ce que viennent de dire les autres témoins?

[*Traduction*]

Leah West: Je comprends certainement la perspective des forces de l'ordre qui souhaitent avoir à leur disposition toutes les données dont elles ont besoin aussi longtemps que nécessaire. Or, en ce qui concerne les protections de la Charte, j'appuie mon opinion sur mes lectures de la jurisprudence européenne sur cette question.

De plus, ce n'est pas seulement le délai d'un an qui pose problème. N'importe quel type de données pourrait être conservé à n'importe quelle fin — même les données relatives à des méfaits ou à des enquêtes sur les traversées illégales, par exemple. Je ne dis pas que c'est ce que feraient les forces policières, mais le fait que tout type de données pourraient être conservées à n'importe quelle fin donne froid dans le dos de la population. En effet, elle pourrait être surveillée alors que toutes ces données seraient conservées aussi longtemps.

En ce moment, rien ne balise la conservation des données: n'importe quel type de données peut être conservé pendant un an, à n'importe quelle fin. Je pense que c'est ce qui doit être amendé pour que la conservation soit plus étroitement adaptée au type de données, aux exigences et aux besoins des enquêtes.

[*Français*]

Claude DeBellefeuille: Si on veut échanger des renseignements avec le Groupe des cinq, ne faut-il pas garder les métadonnées pendant la même période, en moyenne, que celle des pays avec lesquels on collabore?

[*Traduction*]

Leah West: Au sein du Groupe des cinq, les délais varient. Par exemple, en Europe et au Royaume-Uni, seuls les renseignements sur les crimes graves peuvent être conservés pendant un an. Aux États-Unis, les pouvoirs ne permettent pas de conserver les données pendant un an; ce n'est pas prévu dans la loi. Chaque...

[*Français*]

Le vice-président (Frank Caputo): Madame DeBellefeuille, votre temps de parole est malheureusement écoulé.

[*Traduction*]

Monsieur Lloyd, vous avez cinq minutes.

Dane Lloyd (Parkland, PCC): Merci.

Je remercie les témoins de leur présence.

Madame West, l'une des préoccupations que j'ai entendues, c'est que de nombreuses entreprises de technologie disent offrir des contrôles de protection de la vie privée. Par exemple, les entreprises qui vendent des appareils intelligents pour les domiciles disent que les microphones ne peuvent pas être allumés à distance, les empêchant donc d'écouter les utilisateurs. Je trouve un peu étrange qu'on dise que le but du projet de loi n'est pas d'examiner le contenu, mais que des arrêtés ministériels peuvent ordonner aux entreprises de fournir les fonctions pour activer les microphones à distance. Est-ce exact?

Leah West: Là où il est question de contenu, il est en fait question de conservation des données. Le projet de loi permet la création ou l'ordonnance d'une capacité d'interception, et on pourrait donc intercepter les communications. Une ordonnance demandant cette capacité pourrait être émise et, dans la mesure où elle ne créerait pas de vulnérabilité systémique, elle pourrait effectivement être mise en œuvre. Les fournisseurs de service devraient alors modifier leurs publicités.

Dane Lloyd: Cela engendre une situation complexe, car qu'arriverait-il si l'arrêté ministériel était secret?

Leah West: Vous avez raison. Je n'ai pas de réponse à vous donner.

Dane Lloyd: Je ferai un commentaire pour la gouverne du Comité et des personnes qui nous regardent. Disons qu'une entreprise affirme que les microphones ne peuvent pas être activés à distance, puis que le gouvernement émet un arrêté ministériel ordonnant à l'entreprise d'intégrer la fonction pour allumer un microphone à distance. L'entreprise en question ne pourrait alors pas modifier ses publicités pour dire qu'elle n'allumerait pas le microphone sans violer la clause de non-divulgation et de secret. Elle continuerait d'annoncer qu'elle n'allumera pas les microphones à distance alors que le gouvernement l'aurait forcée à créer cette fonction pour les forces de l'ordre.

● (1625)

Leah West: Je ne sais pas comment une entreprise gérerait cette situation.

Dane Lloyd: Je trouve que cela pose problème.

Par ailleurs, je suis préoccupé par la conservation généralisée des métadonnées dont vous avez parlé. Je peux certainement comprendre que si on soupçonne qu'une personne ou un groupe se livre à des activités criminelles, on pourrait ordonner... Je pense que cet outil existe déjà; les ordonnances de conservation existent déjà. Cependant, si on envisage une exigence généralisée selon laquelle les métadonnées de tous les Canadiens et de toutes les personnes qui résident au Canada doivent être conservées pendant une période allant jusqu'à un an, il s'ensuivra de nombreux débats fort intéressants sur le droit constitutionnel en matière de protection de la vie privée... Avez-vous quelque chose à dire à ce sujet?

Leah West: Je suis d'accord avec vous.

J'ai écouté les questions posées lors du dernier témoignage sur la question de savoir si cela constitue ou non une saisie et, si cela ne constitue pas une saisie, si la pratique contreviendrait tout de même à l'article 8. Je pense que cela créerait un profond malaise chez les Canadiens, qui croiraient ne plus avoir de vie privée. En effet, au bout du compte, l'État pourrait avoir accès à tout renseignement concernant un crime commis au cours de la dernière année au moyen d'une ordonnance de communication pour les données de transmission ou d'une ordonnance de localisation, ou même au moyen de données de localisation. L'effet serait paralysant et aurait de graves répercussions sur la perception qu'auraient les gens de leur droit à la vie privée au Canada — et les personnes au Canada ne seraient pas les seules touchées. Toute personne recevant des services d'une entreprise canadienne serait également touchée.

Dane Lloyd: Je ne me préoccupe pas tant des criminels que des personnes innocentes. Je m'inquiète pour les Canadiens innocents dont les métadonnées seront recueillies. Êtes-vous le moindrement préoccupée...?

Nous avons vu le piratage par Salt Typhoon aux États-Unis, alors que des agents étrangers ont piraté des données personnelles de nature très délicate. On a découvert après coup que ce sont les vulnérabilités systémiques exigées par le gouvernement américain qui ont rendu ce piratage possible. Je sais que le but du projet de loi n'est pas de créer des vulnérabilités systémiques, mais je ne suis pas certain que l'accès légal puisse être facilité sans créer... Vous avez dit qu'il y a un risque. Par ailleurs, il est aussi question de forcer les entreprises à conserver les métadonnées des particuliers — de façon généralisée — pour l'ensemble du pays pendant toute une année.

Ne sommes-nous pas en train de créer une mine d'or de données personnelles auxquelles les pirates informatiques voudront avoir accès?

Leah West: Comme je l'ai dit dans ma déclaration préliminaire, tout nouveau point d'accès et tout nouveau bassin de données créent de nouveaux risques, de sorte que le cadre réglementaire...

Le vice-président (Frank Caputo): Je suis désolé. Je dois vous interrompre, madame West.

[*Français*]

Il est difficile de respecter le temps quand nous arrivons aux dernières questions.

[*Traduction*]

C'est difficile, mais juste.

Nous allons écouter le M. Powlowski, qui posera les dernières questions.

[*Français*]

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Ai-je besoin de poser ma question en français?

Des voix: Ha, ha!

Marcus Powlowski: On me dit que ce n'est pas nécessaire.

[*Traduction*]

Monsieur Fleury, je suis heureux de vous voir, même si vous êtes à l'écran. J'ai appris à bien connaître M. Fleury au cours des dernières années. Je dois dire qu'il est un merveilleux chef de police à Thunder Bay. Je suis très heureux que vous soyez parmi nous.

Vous avez donné l'exemple concret d'une fille de 14 ans. Vous pourriez peut-être me dire, lorsque j'aurai terminé de poser cette question assez longue, si c'était un cas réel. J'aimerais en savoir plus sur d'autres cas dont vous vous êtes occupé — vous voudrez peut-être suffisamment dissimuler l'identité des personnes en question — et où l'accès légal vous aurait été utile. Je pense que, dans les cas de pornographie juvénile...

Dans une ville comme Thunder Bay en particulier, il semble y avoir un véritable problème de traite de personnes. Il y a aussi, comme nous le savons tous deux, un gros problème avec les gangs de Toronto et d'Ottawa qui viennent au Canada... eh bien, pas au Canada. Je suppose que Toronto et Ottawa sont aussi au Canada. Ces gangs viennent à Thunder Bay pour commettre des crimes. Les gangs qui font l'aller-retour entre Toronto, par exemple, et Thunder Bay doivent communiquer entre elles.

Pouvez-vous donner d'autres exemples illustrant en quoi l'accès légal vous aiderait à faire votre travail et à régler ces problèmes?

Le chef Darcy Fleury: Le problème bien réel est celui des jeunes qui nous arrivent du Sud. Nous en voyons régulièrement. Certains n'ont que 14 ans. Bien sûr, des parents inquiets communiquent avec nous pour nous demander de l'aide. Au départ, ils s'adressent à la police de Toronto, puis à nous. Ils demandent de l'aide pour retrouver ces enfants.

Dans les faits, l'exploitation de ces jeunes fait en sorte qu'ils se livrent à toutes sortes de crimes et d'activités de gangs. Il nous serait très utile que la loi prévoie un accès plus immédiat. Lorsqu'on commence à déceler les liens entre certains des groupes du Sud et les enfants qui arrivent dans notre région, il serait vraiment utile que nous prenions les devants, surtout lorsque nous recherchons ces jeunes. Nous avons eu des cas réels de familles qui nous ont demandé de l'aide pour partir à la recherche de leurs enfants. Très souvent, nous les trouvons alors qu'ils sont impliqués dans des activités liées à la drogue ou aux gangs qui ont lieu dans notre communauté.

Cela se produit régulièrement. En moyenne, à l'heure actuelle, je dirais que le pourcentage de personnes qui participent à ce type d'activités et qui viennent du Sud de l'Ontario est probablement passé de 60 à 50 %. Je le répète: ces personnes qui commettent des crimes et qui sont exploitées sont très jeunes. Nous nous penchons sur certains de ces cas. Ces jeunes sont-ils victimes de traite de personnes? Ils séjournent dans nos asiles de nuit, et ils finissent par se livrer à toutes sortes d'activités.

Cette situation nous préoccupe vraiment. Je pense que, si nous avions la possibilité d'accéder à l'information un peu plus rapidement, cela nous aiderait certainement à appliquer les lois dont nous sommes responsables.

● (1630)

Marcus Powlowski: Monsieur Fleury, je peux voir comment, dans une situation où des jeunes de 15 ou 16 ans commencent à commettre des délits, on pourrait vouloir avoir accès à leurs données, par exemple sur leur téléphone cellulaire, sur Internet ou dans leurs courriels. C'est souhaitable, mais on peut craindre que ce soit un terrain glissant. Même si c'est peut-être souhaitable, comment puis-je savoir que cela ne suppose pas de surveiller...?

J'ai un garçon de 17 ans. Il a son groupe d'amis. Ils ont des copines. Ils sont toujours en train de socialiser. Comment puis-je savoir que tout ce qu'ils font, y compris parler à Siri, n'est pas transmis à la police? Cela me semble être une atteinte injustifiée à ce que nous considérons comme confidentiel.

Le chef Darcy Fleury: C'est exact. Je pense que les services de police de tout le pays sont très efficaces pour identifier précisément ce qu'ils recherchent. Pour revenir à ma déclaration préliminaire, il ne s'agit pas de mettre en place un champ d'action général et illimité dans lequel la police pourrait obtenir tous les renseignements qu'elle souhaite. Il faut que ce soit directement lié à l'événement qui fait l'objet d'une investigation.

Par exemple, si un jeune est porté disparu dans le Sud de l'Ontario, nous menons une enquête sur la disparition d'un mineur. Par contre, si nous avions accès à ses données et à ses fichiers, cela pourrait immédiatement révéler des liens qui nous permettraient d'élargir la portée de l'enquête pour inclure, par exemple, des contacts et des associés qui se trouvent peut-être à Thunder Bay ou dans le Sud de l'Ontario. Cela nous aiderait à faire avancer notre enquête beaucoup plus rapidement et peut-être à résoudre une partie de la victimisation ou même certaines des activités illégales auxquelles ils pourraient se livrer.

Il s'agirait d'une recherche très ciblée qui ne serait pas ouverte à tous.

Marcus Powlowski: Madame West, puis-je vous poser une question?

Je n'avais pas pensé à quelque chose comme Siri, mais il s'agit de données sur Internet. Si mon fils de 16 ans me demande quelque chose et que je dis à la blague que s'il fait cela, je le battrai avec un bâton de baseball, et que Siri capte ces paroles...

Le vice-président (Frank Caputo): Malheureusement, monsieur Powlowski, c'est la dernière intervention de cette série de questions.

Des députés: Ha, ha!

Le vice-président (Frank Caputo): J'aimerais remercier les témoins d'avoir comparu aujourd'hui.

Anthony Housefather (Mont-Royal, Lib.): Cela commençait juste à devenir intéressant.

Le vice-président (Frank Caputo): Nous allons suspendre la séance pour accueillir les témoins suivants.

● (1630)

_____(Pause)_____

● (1635)

Le vice-président (Frank Caputo): Je vous remercie d'être ici encore une fois pour la deuxième heure.

Nous avons deux témoins dans la salle et un témoin par vidéoconférence. Je crois comprendre que le son de M. Fraser, qui comparaît par vidéoconférence, a été vérifié.

Je vous remercie de votre présence.

Nous accueillons également M. Robert Diab, de l'Université Thompson Rivers.

Enfin, nous accueillons M. Michael Geist, de l'Université d'Ottawa.

Monsieur Diab, pourriez-vous faire votre déclaration préliminaire de cinq minutes?

Robert Diab (professeur, Faculté de droit, Thompson Rivers University, à titre personnel): Merci, monsieur le président et mesdames et messieurs les membres du Comité, de m'avoir invité à comparaître aujourd'hui.

Je suis professeur à la faculté de droit de l'Université Thompson Rivers, et mon domaine de spécialité est l'article 8 de la Charte, qui protège contre « les fouilles, les perquisitions ou les saisies abusives ».

Je tiens d'abord à souligner que le projet de loi C-22 représente une amélioration importante par rapport à son prédécesseur, le projet de loi C-2. En effet, plusieurs des pouvoirs prévus dans le projet de loi ont été mieux adaptés...

Le vice-président (Frank Caputo): Veuillez attendre un instant, s'il vous plaît, monsieur Diab.

Je crois comprendre que nous éprouvons des difficultés.

Anthony Housefather: Je me demandais simplement si M. Diab pouvait parler plus fort, car j'ai du mal à l'entendre.

● (1640)

Robert Diab: D'accord, merci. Je vais essayer.

Anthony Housefather: Merci, monsieur le président.

Le vice-président (Frank Caputo): Je vous remercie.

Robert Diab: Plusieurs des pouvoirs prévus dans le projet de loi ont été mieux adaptés aux besoins des organismes d'application de la loi et aux intérêts en matière de protection de la vie privée, mais j'aimerais présenter brièvement au Comité ce que je considère comme les trois faiblesses importantes qui subsistent dans le projet de loi.

La première concerne les nouvelles ordonnances de communication de renseignements sur les abonnés qui seront ajoutées au Code criminel. Dans son énoncé concernant la Charte, le gouvernement justifie ce pouvoir au motif que les renseignements sur les abonnés ne sont pas particulièrement sensibles, car ils ne révèlent que le nom et l'adresse d'une personne qui obtient un service d'une entité comme Rogers, mais le pouvoir, tel qu'il est rédigé, divulguerait beaucoup plus que cela. En effet, la police peut obtenir non seulement un nom et une adresse liés à un compte, mais aussi les types de services auxquels une personne s'abonne, les forfaits ou les chaînes associés à ces services et les identifiants de chaque appareil associé à ce compte.

Cela s'applique également à toute personne qui fournit un service, et pas seulement à des entreprises comme Rogers. Tout cela permet certainement de saisir des renseignements sensibles comme, par exemple, les forfaits de câblodistribution auxquels une personne est abonnée ou les services médicaux qu'elle reçoit. Le pouvoir d'obtenir ces types de renseignements ne devrait pas reposer uniquement sur des soupçons raisonnables. La portée du pouvoir devrait être restreinte. Dans sa forme actuelle, je pense que cette disposition serait probablement invalidée en vertu de l'article 8.

Deuxièmement, j'aimerais soulever une préoccupation au sujet de la définition des mots « vulnérabilité systémique ». Je crois comprendre que Mme West a abordé le sujet plus tôt, mais je vais tenter de cibler mes commentaires. Il y a une définition, et c'est bien, mais elle est trop restreinte à deux égards.

Le critère de ce qui constitue une vulnérabilité est défini comme ce « qui crée un risque sérieux qu'une personne puisse accéder à de l'information sécurisée sans en avoir le droit ou l'autorisation ». C'est un seuil trop élevé. Les avances en matière d'intelligence artificielle au cours des dernières semaines révèlent son pouvoir beaucoup plus grand en matière de piratage, de sorte que même une vulnérabilité lointaine ou théorique pourrait maintenant être facilement exploitée.

La définition ne s'applique également qu'aux vulnérabilités dans les protections électroniques d'un service électronique. La définition pourrait ne pas s'étendre aux systèmes d'exploitation des appareils, de sorte qu'un arrêté ministériel pourrait, en principe, obliger Apple ou Google à intégrer des capacités d'extraction dans un système d'exploitation sans activer les mesures de protection, même si cela aurait pour effet pratique de compromettre le chiffrement de bout en bout.

La troisième préoccupation concernant le projet de loi est, à mon avis, la plus grave, car il s'agit du pouvoir de conservation des métadonnées, sur lequel le Comité s'est penché il y a quelques minutes. Cela obligerait les fournisseurs principaux à conserver les données de transmission de chaque communication pendant une période maximale d'un an. Cela concerne le moment et l'endroit où nous utilisons nos téléphones et les coordonnées des personnes avec lesquelles nous étions en communication, ainsi que le moment et l'endroit.

L'énoncé concernant la Charte n'aborde pas du tout cette question. Sa position semble être que le fait d'obliger un fournisseur à conserver des métadonnées ne constitue pas en soi une atteinte à la vie privée, car la police a toujours besoin d'un mandat ou d'une autre autorisation pour avoir accès aux données. Cela laisse entendre qu'il ne s'agit pas d'une saisie et que l'article 8 ne s'applique pas, mais ce n'est pas le cas.

Nous savons, grâce à une abondante jurisprudence, que les métadonnées relèvent de la vie privée, et en vertu de ces dispositions, lorsque le ministre oblige Shaw ou Telus à conserver nos métadonnées, l'entreprise le fait au nom de l'État et à des fins d'application de la loi. Ce sont des éléments fondamentaux d'une saisie en vertu de l'article 8.

Il convient de souligner que c'est précisément ce que le Parlement a présumé il y a 12 ans, lorsqu'il a ajouté au Code criminel le pouvoir d'émettre une demande ou une ordonnance de conservation, ce qui exige des soupçons précis, des soupçons raisonnables ou un mandat, selon le cas. C'est un élément essentiel, car il érige en infraction criminelle le fait de détenir des données, dans le cas de Shaw ou Telus ou toute autre entité, au-delà de la période prévue. Pourquoi le Parlement aurait-il présumé qu'une autorisation était nécessaire pour conserver des données si l'article 8 ne s'appliquait pas?

Rien ne change dans ce cas-ci, selon moi, parce que la police affirme qu'elle n'examinera pas les données à moins d'obtenir un mandat. C'est aussi le cas à l'heure actuelle. Pour voir les données dont la conservation est exigée, elle a besoin d'un mandat, mais la conservation elle-même est...

Le vice-président (Frank Caputo): Je vous remercie, monsieur Diab.

Au Parlement, nous sommes habitués à ce que les interventions soient écourtées, et je m'excuse donc de vous avoir interrompu.

J'aimerais également souhaiter la bienvenue à Mme Kayabaga et à M. Baber.

Monsieur Geist, veuillez faire votre déclaration préliminaire. Vous avez cinq minutes.

● (1645)

Michael Geist (titulaire de la Chaire de recherche du Canada en droit de l'Internet et du commerce électronique, professeur de droit, Faculté de droit, Université d'Ottawa, à titre personnel): Bonjour tout le monde. Je vous remercie de l'invitation à comparaître.

Comme vous l'avez entendu, je m'appelle Michael Geist. Je suis professeur de droit à l'Université d'Ottawa, où je suis titulaire de la Chaire de recherche du Canada en droit de l'Internet et du commerce électronique. Je comparais à titre personnel et je n'exprime que mes propres opinions.

En me préparant pour la séance d'aujourd'hui, j'ai passé en revue mes antécédents dans le domaine de la politique sur l'accès légal. J'ai constaté que j'avais écrit ma première lettre d'opinion sur la question il y a plus de 20 ans et que j'avais commencé à comparaître pour la première fois devant des comités, au sujet de divers projets de loi, quelques années plus tard.

Comme vous le savez sans doute, l'accès légal fait l'objet de débats législatifs au Canada depuis des décennies, tant sous les gouvernements libéraux que conservateurs. Les technologies évoluent et les gouvernements peuvent se succéder, mais le défi a toujours été le même, à savoir donner aux organismes d'application de la loi et de sécurité les outils dont ils ont besoin pour lutter contre les crimes graves tout en respectant le droit à la vie privée des Canadiens et le cadre constitutionnel que la Cour suprême a établi en matière de protection de la vie privée dans des décisions comme l'arrêt Spencer et l'arrêt Bykovets.

Le projet de loi C-2 illustre ce qui se passe lorsqu'un équilibre n'est pas atteint, car son pouvoir d'exiger des renseignements sans mandat prévoyait la divulgation obligatoire des renseignements sur les abonnés de tout fournisseur de services au Canada, sans surveillance judiciaire. La décision d'abandonner ce pouvoir était judicieuse, et son remplacement par une demande de confirmation de service est un changement utile. Le projet de loi C-22 présente néanmoins de graves problèmes, et je vais me concentrer sur trois d'entre eux. Ils font écho à ce que nous venons d'entendre de la part de M. Diab.

Tout d'abord, je vais m'attarder sur le régime de conservation obligatoire des métadonnées, qui obligerait les fournisseurs à conserver les métadonnées de chaque abonné pendant un an, indépendamment de tout soupçon. Sur un réseau de téléphonie mobile, ces données comprennent les relais de téléphone cellulaire auxquels chaque téléphone se connecte. À grande échelle, l'ensemble de ces données constitue une carte de surveillance complète de presque tous les Canadiens qui indique où et quand ils se déplacent et avec qui ils interagissent. C'est le type de régime de conservation massive des données que la Cour de justice de l'Union européenne a invalidé dans l'affaire Digital Rights Ireland et qui, dans l'affaire Tele2 Sverige, s'étendait à l'obligation pour le secteur privé de conserver les données de circulation et de localisation. La Cour constitutionnelle fédérale allemande est parvenue à des conclusions semblables, mais il convient de souligner que l'énoncé concernant la Charte au sujet du projet de loi C-22 ne mentionne pas ce régime, malgré ses répercussions évidentes sur la Charte.

On demande au Comité d'enchâsser une architecture de surveillance et d'accepter les risques de sécurité qui en découlent. L'approche évidente consiste à supprimer complètement cette disposition, car elle est disproportionnée et, je crois, susceptible d'être invalidée dans sa forme actuelle par la Cour suprême. Par ailleurs, une limite de 30 jours sur la conservation des métadonnées suffirait peut-être pour répondre aux besoins immédiats en matière d'enquête, tout en permettant une ordonnance du tribunal si une période plus longue est nécessaire.

La deuxième préoccupation concerne les mesures de protection contre la vulnérabilité systémique dans les dispositions relatives aux capacités techniques. Les articles 5 et 7 proposés de la Loi sur le soutien en matière d'accès autorisé à de l'information — dans la partie 2 — stipulent que les fournisseurs ne sont pas tenus de se conformer à une ordonnance si cela introduit une « vulnérabilité systémique ». Les articles 12 et 13 proposés rendent la conformité inconditionnelle et prévoient que les ordonnances l'emportent sur les règlements incompatibles. Il en résulte une mesure de protection qui n'existe que de nom et qui est largement voilée par le secret, et il incombe aux fournisseurs de l'invoquer. Cela se traduit par une obligation de créer des moyens détournés qui pourraient affaiblir le chiffrement, mettre en péril les données des utilisateurs et amener les entreprises à retirer du Canada les services qui améliorent la protection de la vie privée.

Il faut corriger cette situation, notamment en modifiant l'article 12 proposé pour que la conformité soit assujettie aux dispositions des articles 5 et 7 proposés. De plus, la définition de « vulnérabilité systémique » devrait être élargie par la loi, en précisant qu'il ne sera pas nécessaire d'affaiblir ou de contourner le chiffrement ou d'introduire une quelconque faiblesse en matière de sécurité.

La troisième préoccupation concerne le seuil requis pour les ordonnances de communication de renseignements sur les abonnés. Le projet de loi C-22 fixe la norme aux « motifs raisonnables de soupçonner » plutôt qu'à la norme actuelle liée aux « motifs raisonnables de croire ». Les décisions Spencer et Bykovets établissent un intérêt élevé en matière de protection des renseignements personnels concernant les données des abonnés, mais l'énoncé concernant la Charte affirme néanmoins que « [l]es renseignements relatifs à l'abonné ne constituent pas en eux-mêmes des renseignements particulièrement sensibles ». Je pense que cette phrase est difficile à concilier, tant avec la jurisprudence de la Cour suprême qu'avec la réalité technique de ce que les renseignements sur les abonnés peuvent révéler. L'abaissement du seuil invite d'autres contestations fondées sur la Charte, ce qui affaiblit la disposition sur le plan juridique.

Aucun des changements dont j'ai parlé ici ne serait incompatible avec des outils d'application de la loi efficaces. Il s'agit plutôt de garantir un cadre qui peut résister à l'examen fondé sur la Charte, respecter les droits à la vie privée des Canadiens, éviter de créer une infrastructure de surveillance et préserver l'intérêt public et la confiance de la population.

● (1650)

Je me ferai un plaisir de répondre à vos questions.

Le vice-président (Frank Caputo): Je vous remercie, monsieur Geist.

La parole est maintenant à M. Fraser. Il a cinq minutes.

David Fraser (associé, McInnes Cooper, à titre personnel): Monsieur le président et mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invité à vous faire part de mon point de vue sur le projet de loi C-22.

Je suis associé au sein du cabinet d'avocats McInnes Cooper, à Halifax, où je conseille notamment des clients qui sont visés par des ordonnances de communication de renseignements sur la clientèle. J'enseigne également à la faculté de droit de l'Université Dalhousie. Je comparais à titre personnel et je présente mes propres points de vue. Je ne parle au nom d'aucun de mes clients.

Je dois féliciter le gouvernement pour les vastes consultations qu'il a menées auprès des intervenants depuis le projet de loi C-2, auquel j'ai contribué, mais j'ai encore un certain nombre de préoccupations et de recommandations. Je tiens en particulier à souligner que la partie 2 du projet de loi C-22 est très problématique. Je ne peux pas aborder toutes mes préoccupations en cinq minutes, et j'attends donc avec impatience la suite de notre discussion.

Tout d'abord, je suis d'accord avec mes collègues. Nous devons restreindre la portée des ordonnances de communication de renseignements sur les abonnés ou relever le seuil à celui de la croyance raisonnable. Le projet de loi abaisse le seuil à partir duquel la police peut obtenir une ordonnance de communication de renseignements sur les abonnés — ce qu'elle peut obtenir aujourd'hui — de « motifs raisonnables de croire » à « motifs raisonnables de soupçonner ».

Toute entité fournissant des services à la population, notamment les banques, les hôpitaux, les épiceries et les hôtels, serait susceptible d'être visée par ces ordonnances. Nous avons largement dépassé les entreprises de télécommunications. Même si la définition est plus étroite que dans les projets de loi précédents, la police pourrait toujours exiger tous les renseignements sur les abonnés détenus par un fournisseur de services. Cela irait au-delà du nom et de l'adresse, comme mes collègues l'ont souligné. Il s'agirait notamment des types de services fournis et des identifiants des appareils, comme le numéro de série de l'appareil de ventilation en pression positive continue dans le cabinet de votre médecin. Cela obligerait Apple à communiquer les identifiants numériques de tous vos appareils, y compris vos AirTag et vos iPad. C'est excessif. Je suggère de restreindre la portée de ces ordonnances ou de relever le seuil à la croyance raisonnable. Dans le cas contraire, on finira par conclure qu'il s'agit d'une violation de la Charte.

J'aimerais maintenant aborder la partie 2, qui édicte la Loi sur le soutien en matière d'accès autorisé à de l'information.

Personne n'a présenté d'arguments convaincants concernant quoi que ce soit dans la partie 2. Le gouvernement a eu plus de 20 ans pour constituer son dossier, mais comme l'a fait remarquer le Comité des parlementaires sur la sécurité nationale et le renseignement, il ne dispose que d'anecdotes. Nous ne devrions pas porter atteinte à la vie privée et à la sécurité des Canadiens sur le fondement d'anecdotes.

La partie 2 du projet de loi vise les fournisseurs de services électroniques, mais la définition est tellement vaste qu'elle inclurait probablement la plupart des entreprises au Canada. Tout le monde utilise des renseignements numériques. S'il est adopté, le projet de loi devrait prévoir les mesures de protection nécessaires. Le gouvernement ne devrait en aucun cas être autorisé à exiger — en particulier par l'entremise d'une ordonnance secrète — qu'un fournisseur de services électroniques apporte des changements aux produits ou aux services qu'il fournit dans le cadre normal de ses activités, qu'il collecte et conserve des données au-delà de ce dont l'entreprise a besoin pour ses propres besoins ou qu'il apporte tout changement qui aurait une incidence sur la fonctionnalité, y compris l'ajout de fonctionnalités supplémentaires pour tout produit ou service offert par l'entreprise. Selon le libellé actuel du projet de loi, le ministre de la Sécurité publique pourrait prendre un décret secret pour transformer un appareil Alexa d'Amazon en dispositif d'écoute, comme dans un exemple donné par le groupe de témoins précédent. Le SCRS a expressément indiqué, à propos de ce projet de loi, qu'il souhaitait pouvoir suivre en temps réel chaque téléphone cellulaire au Canada et que les entreprises de télécommunications devraient modifier leurs services pour permettre le suivi de chaque téléphone cellulaire. Il s'agirait là d'une mesure disproportionnée et, à mon avis, absurde.

Maintenant, le gouvernement dit qu'il n'a pas l'intention de compromettre le chiffrement et qu'il n'y aurait pas de moyens détournés, mais il suffit de lire le libellé du projet de loi pour constater qu'il ne contient rien pour empêcher cela. Des représentants du gouvernement ont déclaré devant le Comité — je crois que c'était mardi — que le projet de loi est « neutre en ce qui concerne le chiffrement », mais les Canadiens ne sont pas neutres en ce qui concerne le chiffrement. Le libellé du projet de loi permettrait clairement — et n'interdirait certainement pas — le déchiffrement par des moyens détournés et le déchiffrement obligatoire. Cela se ferait en secret, sans transparence pour les Canadiens et sans grande reddition de comptes. L'intention du gouvernement importe peu. Ce qui importe, c'est le libellé de la loi.

En vertu de la partie 2, le ministre de la Sécurité publique pourrait émettre des ordonnances secrètes visant des fournisseurs de services électroniques — au sens très large — qui s'accompagnent d'une obligation au secret à perpétuité. À l'heure actuelle, la police et le SCRS peuvent demander à un juge ce qu'on appelle une ordonnance d'assistance, qui oblige un fournisseur de services à fournir toute l'aide raisonnable pour exécuter un mandat judiciaire. Elle peut être accompagnée d'une ordonnance de non-divulgation si on juge que c'est nécessaire. Cela revient à exercer un contrôle judiciaire. Aucun représentant des forces de l'ordre n'a fourni de preuves selon lesquelles les ordonnances d'assistance sont inadéquates ou devraient être remplacées par ces arrêtés ministériels secrets. L'équivalent britannique d'un arrêté ministériel a été utilisé par le gouvernement britannique pour ordonner secrètement à Apple de supprimer le chiffrement sur iCloud de façon générale. La partie 2 du projet de loi C-22 ne contient aucune mesure de protection qui empêcherait un tel abus de pouvoir au Canada. Les arrêtés ministériels secrets doivent disparaître.

Il y a aussi la question de la conservation des métadonnées, que mes collègues ont déjà abordée. Cela comprendrait l'historique des déplacements. Ainsi, le gouvernement pourrait exiger que le téléphone cellulaire de chaque personne devienne un dispositif de suivi rétrospectif remontant jusqu'à un an en arrière, sans aucun soupçon d'acte répréhensible. Cela sera presque certainement jugé contraire à la Charte. Les autorités canadiennes et non canadiennes tenteraient de collecter des métadonnées sur le fondement de simples soupçons. Il s'agirait par exemple d'un registre de toutes les personnes qui ont demandé des soins de santé génésique au Canada, ce qui pourrait intéresser les forces de l'ordre d'un pays partenaire du Groupe des cinq.

● (1655)

Enfin, pendant qu'un nombre considérable d'experts en cybersécurité...

Le vice-président (Frank Caputo): Je suis désolé, monsieur Fraser, mais nous allons devoir nous arrêter ici. Je m'en excuse.

David Fraser: Je vous remercie.

Le vice-président (Frank Caputo): À titre de président, je vais mener cette prochaine série de questions de six minutes.

Je tiens à remercier tous les témoins. Nous avons un groupe de témoins très érudits aujourd'hui. Je suis honoré que vous nous ayez tous les trois accordé votre temps aujourd'hui. Avez-vous remarqué que nous sommes tous des avocats? C'est merveilleux.

Monsieur Diab, c'est formidable de vous avoir ici en tant que collègue avec qui j'ai travaillé au Barreau de la Colombie-Britannique lorsque j'étais procureur et aussi lorsque j'enseignais le droit pénal avancé et la détermination de la peine à l'Université Thompson Rivers. Je sais que tout le monde est très fier de vous accueillir parmi nous, et je vous remercie de votre présence.

J'aimerais maintenant approfondir la question de l'application de l'article 8 en ce qui concerne l'obligation pour un tiers de conserver des données. Vous appuyez-vous sur un cas précis, monsieur?

Robert Diab: Non, je m'appuie simplement sur les principes généraux de l'article 8. L'article 8 s'applique lorsqu'un acteur étatique porte atteinte à un élément pour lequel nous avons un intérêt raisonnable en matière de protection de la vie privée. Je crois donc comprendre que votre question concerne la simple demande d'un agent de l'État à l'égard d'un tiers de conserver des données privées appartenant à une personne donnée. Est-ce une atteinte à sa vie privée? Encore une fois, il y a 12 ans, le Parlement a présumé que, si un tribunal devait se pencher sur la question, il conclurait que cela porte atteinte à sa vie privée.

Autrement dit, je ne vois pas de jurisprudence où la police aurait demandé à des tiers de conserver des données et où cela aurait ensuite été contesté devant les tribunaux. Un tel cas ne me vient pas à l'esprit. Pour moi, tout commence par ce pouvoir, c'est-à-dire le pouvoir de conservation, et lorsqu'il a été ajouté au Code, je présume que c'était en partant du principe que le fait d'exiger d'un tiers qu'il agisse ainsi pour le compte de l'État à des fins d'application de la loi constitue une atteinte relevant de l'article 8.

Encore une fois, prenez du recul et demandez-vous comment vous vous sentiriez si on vous disait que Telus, Rogers et d'autres entreprises conservent un registre de tous vos déplacements et des personnes à qui vous avez envoyé des courriels — non pas le contenu, mais tous ces détails. Comment vous sentiriez-vous? Ces données seraient conservées pendant une période pouvant aller jusqu'à un an, afin de pouvoir vous poursuivre au besoin.

Peut-être que quelqu'un répondra que cela ne lui pose aucun problème, mais je pense que la plupart des Canadiens et, selon moi, les tribunaux, ne seraient pas de cet avis. Ils estimeraient que le simple fait que j'ai rendu visite à une personne un certain jour ou que j'ai parlé à une autre personne un autre jour relève de la vie privée. Ces renseignements devraient rester confidentiels. Ils ne devraient pas être conservés dans un registre, et c'est, à mon avis, la meilleure explication que je puisse vous donner pour justifier cela.

Le vice-président (Frank Caputo): Je vous remercie.

J'aimerais demander aux deux professeurs qui sont dans la salle ce qu'ils pensent des motifs raisonnables de soupçonner par rapport aux motifs raisonnables de croire. Il y a un certain temps que je n'ai pas traité des motifs raisonnables de soupçonner, mais si je me souviens bien, les motifs raisonnables de croire doivent reposer sur une croyance subjective, c'est-à-dire qu'il faut personnellement croire qu'une infraction a été commise, et cette croyance doit être objectivement raisonnable. C'est ce dont je me souviens. Autrement dit, une personne raisonnable considérerait qu'il y a des motifs raisonnables de croire qu'il y a infraction.

C'est en dessous du seuil de la prépondérance des probabilités, et ce n'est donc pas extrêmement élevé. C'est moins de 50 %, mais supérieur au simple soupçon, ce qui est plus qu'une intuition, mais moins que cela.

Que pensez-vous de l'argument selon lequel cela ne concerne que des données très restreintes et que, par conséquent, nous n'avons pas à nous inquiéter outre mesure que cela puisse être sauvegardé en vertu de l'article 1?

Êtes-vous d'accord, monsieur Geist?

Michael Geist: Non, je ne suis pas d'accord pour deux raisons.

Tout d'abord, l'affirmation récurrente selon laquelle ces données présentent un faible intérêt en matière de protection de la vie privée est, à mon avis, tout simplement inexacte. Nous venons d'entendre les exemples cités par M. Diab et nous aurons peut-être l'occasion, au cours des prochaines minutes, de passer en revue certains de ces exemples, mais il me semble que, même avec la question soulevée à la fin de la comparution de votre dernier groupe de témoins, à savoir si quelqu'un pourrait savoir que vous avez posé une question à Siri, la question n'est pas le contenu. Le fait est que vous l'avez soulevée et que vous avez interagi avec des personnes. Le fait est que des membres du public communiquent avec vous et qu'il existerait une liste des personnes avec lesquelles vous avez communiqué. Le fait que des ordonnances puissent être rendues pour que ces types de renseignements soient divulgués soulève, de mon point de vue, des questions importantes.

Cela pourrait avoir des implications importantes pour la protection de la vie privée, et revoir à la baisse le seuil applicable à la divulgation de ces renseignements, lorsqu'il n'y a guère de preuves que le seuil plus élevé que nous avons en place depuis de nombreuses années pose problème, me semble injustifié.

● (1700)

Le vice-président (Frank Caputo): D'accord.

J'aimerais m'adresser à M. Fraser, qui comparaît en ligne. J'ai mentionné à la dernière réunion, lorsque je n'étais pas président, qu'il s'agit d'un projet de loi très technique. Nous n'avions eu qu'une heure avec les fonctionnaires.

J'aimerais aborder un point que vous avez soulevé devant le Comité. Vous avez dit que le SCRS souhaitait disposer d'un accès en temps réel. Je pense que le Comité voudra peut-être interroger le SCRS à ce sujet.

Pour notre gouverne et celle de nos analystes, pouvez-vous nous dire d'où vous tenez ce renseignement, s'il vous plaît, en 25 secondes ou moins?

David Fraser: Oui, certainement. Ce point a été soulevé dans le cadre de la séance d'information technique lors du dépôt du projet de loi. Il en a été question pour le projet de loi C-2 et de nouveau pour le projet de loi C-22. J'ai un exemplaire de la présentation avec la diapositive qui contient l'illustration, si vous souhaitez la consulter.

Le vice-président (Frank Caputo): Je suis sûr que nous l'avons aussi.

Il me reste 10 secondes, mais nous avons un peu de retard, et nous allons donc passer à M. Housefather.

Je vous remercie.

Anthony Housefather: Je vous remercie, monsieur le président. Ces 10 secondes seront certainement très importantes pour terminer la réunion plus tôt.

Des députés: Ha, ha!

Anthony Housefather: C'est un plaisir d'accueillir les témoins.

Dans tous les différents groupes de témoins, nous observons une tension générale entre...

[*Français*]

Claude DeBellefeuille: J'invoque le Règlement.

[*Traduction*]

Le vice-président (Frank Caputo): Nous avons un rappel au Règlement.

[*Français*]

Claude DeBellefeuille: Je pense que la majorité des gens ne portent pas d'oreillette pour l'interprétation. C'est très difficile pour moi aujourd'hui, parce que toutes les discussions sont en anglais. Je ne fonctionne qu'avec l'interprétation. J'aime beaucoup M. Housefather, mais il parle très vite.

Pourrait-il ralentir le débit pour que je puisse suivre ses questions?

Je suis certaine qu'elles seront intéressantes.

Anthony Housefather: Absolument, je vais parler moins vite.

Claude DeBellefeuille: Merci, monsieur Housefather.

[*Traduction*]

Un député: Et nous venons de perdre l'avance de 10 secondes.

[*Français*]

Le vice-président (Frank Caputo): Merci, monsieur Housefather.

Anthony Housefather: Je vais parler moins vite.

Claude DeBellefeuille: Je ne veux pas vous enlever du temps de parole.

[*Traduction*]

Anthony Housefather: Encore une fois, je vous remercie d'être ici aujourd'hui.

Je pense qu'il y a une tension générale dans cette loi, comme vous l'avez souligné à juste titre, entre l'objectif d'assurer la plus grande sécurité possible et celui de respecter le droit à la vie privée. Nous devons trouver un juste milieu qui convient à la majorité des gens. Je ne pense pas que nous parviendrons un jour à une situation où tout le monde s'entendra sur les détails du projet de loi, mais je pense que nous devons essayer de trouver un compromis raisonnable.

Nous partons du principe que le projet de loi est louable en ce sens qu'il corrige certaines des lacunes du projet de loi C-2. Le projet de loi est nécessaire pour permettre aux forces de l'ordre d'avoir accès à des renseignements qui, sur le plan technologique, ne sont pas couverts par la loi actuelle, mais comme tout le monde ici, vous avez exprimé certaines préoccupations.

J'ai observé qu'on n'était pas à l'aise avec l'idée de prendre certains règlements à cet égard. Je tiens à souligner que le contenu de ces règlements suscite une certaine méfiance, et nous entendons ensuite des hypothèses sur ce qu'ils pourraient contenir ou sur la façon dont les ordonnances pourraient être utilisées. Certaines personnes feront confiance au gouvernement en affirmant qu'il agira de façon raisonnable, que la Charte s'applique toujours et qu'un contrôle judiciaire est toujours exercé. D'autres affirment qu'ils ne lui feront pas confiance à moins que ce soit écrit dans le projet de loi. Je conçois tout cela.

J'ai également exprimé des préoccupations au sujet de l'interaction entre les vulnérabilités systémiques et les ordonnances. Selon mon interprétation du projet de loi, l'entreprise n'est pas tenue de se conformer si cela crée une vulnérabilité systémique. Je comprends qu'il faudra peut-être se pencher sur la définition de la vulnérabilité systémique. Cependant, l'entreprise est tenue de se conformer à une ordonnance.

Monsieur Geist, vous avez abordé cet enjeu. Pourriez-vous nous dire comment vous modifieriez le projet de loi pour régler ce problème?

Michael Geist: J'aimerais souligner deux ou trois points.

Tout d'abord, il est essentiel de préciser cet enjeu à l'aide d'une définition plus détaillée. De nombreuses personnes ont exprimé des préoccupations sur ce que cela pourrait signifier et sur les conséquences, qui pourraient être graves en ce qui concerne notre cybersécurité et la vie privée des gens. Je pense donc que nous devons, pour le bien de tous, apporter davantage de précisions.

Avec tout le respect que je vous dois, je pense que les gens ont de bonnes raisons d'écouter le débat et de penser que certaines de ces préoccupations sont certainement justifiées. Par exemple, pendant le débat à la Chambre, j'ai entendu la secrétaire d'État (Lutte contre la criminalité) dire que c'était une première étape. Je suis arrivé à l'audience juste avant cela, et les agents de police disaient vouloir des métadonnées pendant deux ou trois ans. La prochaine étape consistera-t-elle à prolonger cette période de plusieurs années? Je ne sais pas, mais cela soulève de réelles préoccupations.

Pour répondre à votre question, nous avons besoin d'une définition beaucoup plus précise pour indiquer très clairement que cela ne touchera pas le chiffrement et qu'aucune ordonnance ne créera des faiblesses systémiques. C'est un point de départ clair.

● (1705)

Anthony Housefather: On dit toutefois, en substance, que les articles 5 et 7 proposés sont assujettis à l'article 10 proposé. Je comprends également qu'il faut revoir la définition de « vulnérabilité systémique ».

Michael Geist: Oui, c'était mon autre point. Il y en avait deux, soit la définition et ensuite l'incohérence dans le projet de loi qui évoque, d'une part, la capacité de soulever des préoccupations, mais d'autre part, utilise un libellé qui laisse entendre qu'on n'a pas vraiment la capacité de contester ou, à tout le moins, d'éviter une ordonnance.

Anthony Housefather: Je suis très sensible à cette question.

Je tiens à mentionner quelque chose, car je suis moins d'accord pour passer des « motifs raisonnables de soupçonner » aux « motifs raisonnables de croire ». Je tiens à souligner que les « [c]onditions préalables à l'ordre » indiquent ce qui suit:

> (2) L'agent de la paix ou le fonctionnaire public ne donne l'ordre que s'il a des motifs raisonnables de soupçonner, à la fois:
>
> a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;
>
> b) que la confirmation visée par l'ordre sera utile à l'enquête relative à l'infraction.

Je pense que cette combinaison crée effectivement une situation où il existe un fardeau raisonnable, déterminé par l'ensemble des circonstances, qui rend ce seuil relativement raisonnable dans ce contexte.

Je comprends toutefois l'idée de limiter la portée de l'ordonnance de communication de renseignements, mais si nous faisions cela, devrait-elle concerner, par exemple, le nom et l'adresse d'une personne — tout ce qu'on pouvait autrefois trouver dans l'annuaire téléphonique — et pas nécessairement tous les services qu'une personne a reçus, par exemple? Seriez-vous d'accord, dans ce cas, pour dire qu'il s'agit d'un seuil raisonnable?

Cette question s'adresse à vous, monsieur Diab, car je l'ai déjà posée à M. Geist.

Robert Diab: Je vous remercie de la question.

Je pense qu'il y a deux parties à cela.

Tout d'abord, en ce qui concerne le libellé que vous avez cité au début, le préambule, il s'agit d'un libellé standard. Lorsqu'il sera contesté et que les tribunaux évalueront s'il s'agit d'une loi raisonnable en vertu de l'article 8 proposé, ils en examineront la portée en plus des motifs. Une partie de toute la question est la suivante: le soupçon « raisonnable » est-il trop faible, ne serait-ce que pour le nom et l'adresse de l'abonné? C'est une question qui reste ouverte dans la foulée de l'arrêt *Spencer* .

Pour reprendre un point que M. Geist a soulevé il y a quelques minutes, dans l'arrêt *Spencer*, la Cour a dit que nous avons un intérêt « élevé » en matière de protection de la vie privée dans le nom associé à nos renseignements d'abonnés, parce que cela nous relie à tout un historique de recherche. C'est un intérêt élevé. Ce n'est pas ce que la cour a dit. Elle insinuait que rien de moins qu'un mandat pour des motifs probables serait raisonnable, mais on ne lui a pas posé cette question et elle n'a pas eu à répondre...

Frank Caputo: Je suis désolé, monsieur Diab, mais je dois vous interrompre.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille: Merci, monsieur le président.

Monsieur Geist, vous nous avez dit que, conserver les métadonnées pendant un an, c'était trop, et que 30 jours, ce serait une période raisonnable. Vous avez précisé que, si on a des doutes raisonnables de croire qu'il y a des motifs criminels, il faut obtenir un mandat pour prolonger la durée de conservation.

Ai-je bien compris votre recommandation à ce sujet?

[*Traduction*]

Michael Geist: Oui. C'est ce que je proposais.

En un sens, ce que j'essayais de dire, c'est que les forces de l'ordre ont toujours la capacité, si elles ont besoin de ces renseignements dans le cadre d'une longue enquête en cours, de demander l'ordonnance nécessaire pour les préserver. Je pense que le problème que les forces de l'ordre ont cerné dans ce contexte, c'est qu'on ne sait pas ce qu'on ne sait pas dans certaines circonstances, alors on ne sait pas si on pourrait en avoir besoin. Il y a ce désir de construire cette énorme botte de foin d'information, parce que vous aurez peut-être besoin de l'aiguille à un moment donné.

Il me semble que, bien sûr, la botte de foin est composée de gens qui n'ont rien fait de mal. Ils n'ont aucun soupçon contre eux. Cela soulève pour eux de réelles préoccupations liées à la vie privée. Y a-t-il un mécanisme que nous pouvons trouver, dans le but de répondre aux préoccupations des organismes d'application de la loi, qui permettra, sur une base continue, de conserver une partie de ces renseignements, mais de les éliminer rapidement après une période appropriée?

Dans le dernier groupe de témoins, j'ai entendu, je crois, l'un des membres des forces de l'ordre à qui on a demandé un cas d'utilisation et qui a parlé d'une personne disparue. Ne serait-il pas bon de pouvoir obtenir cette information? Avec tout le respect que je vous dois, vous n'avez pas besoin de conserver les métadonnées de tout le monde pendant un an pour quelqu'un qui a disparu. Franchement, je pense que 30 jours sont plus que suffisants pour se rendre compte que la personne est portée disparue. Ensuite, si on a besoin d'essayer d'obtenir d'autres métadonnées, on peut obtenir l'ordonnance pour les consulter.

● (1710)

[*Français*]

Claude DeBellefeuille: Monsieur Geist, je vous remercie de votre réponse. C'est assez clair.

Vous savez que le projet de loi C-22 nous tient à cœur, ici. Nous avons tous pris l'engagement de collaborer et, surtout, de l'améliorer. Alors, si vous avez un amendement à proposer ou une indication particulière à nous donner pour l'améliorer, je vous invite à nous en faire part. Toutes vos suggestions sont les bienvenues, surtout si vous nous les communiquez dans les deux langues officielles. Elles vont être acheminées rapidement aux membres du Comité.

Je vais maintenant vous poser mon autre question.

À moins que j'aie mal compris, j'ai appris qu'en Europe, la conservation des données se limite aux cas de crimes graves, et que l'Europe est beaucoup plus précautionneuse quant à la protection de la vie privée. Aux États-Unis, ce n'est pas très clair non plus si les métadonnées sont conservées pour une très longue période.

Considérez-vous que le Canada, dans le projet de loi C-22, est plus intrusif que ses partenaires du Groupe des cinq quant à la conservation des métadonnées?

[*Traduction*]

Michael Geist: L'Europe a eu toute une série de cas, tant au niveau européen qu'au niveau national dans un certain nombre d'États membres, qui ont conclu que certaines initiatives relatives à la conservation obligatoire des métadonnées étaient disproportionnées. Il y a ces cas, et les pays commencent à réagir. Il y a un peu de confusion en ce qui concerne la durée, les circonstances et les cas particuliers dans lesquels on pourrait être en mesure de conserver ces renseignements, mais il est très clair que les tribunaux européens ne sont pas à l'aise avec ce que j'appellerais maintenant le projet de loi C-22 — l'approche des métadonnées — qui consiste à tout conserver pendant un an. Comme vous l'avez entendu dans le dernier groupe de témoins, nous ne voyons pas du tout cette conservation aux États-Unis. De toute évidence, cela nous met en décalage par rapport à certains de ces pays, mais peut-être plus important encore, aux fins de la création d'une loi qui résistera à une contestation potentielle, je pense que cela ne correspond pas à la Charte.

[*Français*]

Claude DeBellefeuille: Les membres des forces de l'ordre et du gouvernement qui ont témoigné ou qui nous ont interpellés nous ont dit qu'ils voulaient s'aligner sur les normes du Groupe des cinq. Maintenant, selon ce que je comprends, vous nous dites que la mesure qui prévoit la captation et la conservation des données pendant un an est plus sévère et plus exigeante que ce qu'on voit dans les pays du Groupe des cinq et, à plus forte raison, en Europe.

Ai-je bien compris, monsieur Geist?

[*Traduction*]

Michael Geist: Vous pouvez trouver des exemples où c'est cohérent, ou autre chose. Encore une fois, juste avant la discussion, nous avons entendu parler de nombreux problèmes liés à la criminalité dans l'axe nord-sud. Aux États-Unis, nous ne voyons pas ces exigences en matière de métadonnées. Dans de nombreux pays européens, nous ne les voyons pas non plus. Le Canada serait certainement disposé à créer un système sans cela ou, s'il le faisait, pour une très courte période, en travaillant de concert avec la capacité d'obtenir rapidement des ordonnances de gel rapide pour s'assurer que vous pouvez conserver les données plus longtemps. Je vois peu de raisons de penser que cela ne serait pas considéré comme faisant notre part par rapport à nos alliés.

[*Français*]

Claude DeBellefeuille: Pourquoi pensez-vous, professeur Geist, que le gouvernement, dans sa définition concernant les fournisseurs de services électroniques, veut se laisser beaucoup de liberté sur le plan réglementaire?

Pourquoi veut-il garder ce pouvoir, d'après vous?

[*Traduction*]

Michael Geist: J'aimerais avoir une bonne réponse. J'ai mentionné d'entrée de jeu que c'est une question sur laquelle je me concentre depuis des décennies. D'après mon expérience, les gouvernements des deux partis, peu importe qui est au pouvoir, lorsqu'ils travaillent avec les forces de l'ordre pour étoffer cela...

● (1715)

[*Français*]

Le vice-président (Frank Caputo): Je suis désolé, madame DeBellefeuille et professeur Geist.

[*Traduction*]

Le temps est écoulé.

Madame Kirkland, votre temps de parole commence maintenant. Vous avez cinq minutes.

Rhonda Kirkland: Merci, monsieur le président.

Monsieur Fraser, je vous remercie d'être ici aujourd'hui. Mes premières questions s'adresseront à vous.

Permettez-moi de commencer par la différence entre ce qui est prévu et ce qui est permis. Je pense que la plupart des Canadiens ne contesteraient pas l'intention de ce projet de loi. Souvent, lorsque nous posons des questions au ministère de la Justice et à celui de la Sécurité publique, ils se fient à l'affirmation suivante: « Eh bien, ce n'est pas l'intention de ce projet de loi ». Ma préoccupation est plutôt la suivante: qu'est-ce que cela permet de faire par rapport à l'intention du projet de loi?

Hier, Sécurité publique Canada, sur la plateforme de réseaux sociaux X, a publié ceci: « Fait ou Fiction? Le projet de loi C-22 obligera les fournisseurs de services électroniques à créer des moyens détournés de contourner leurs systèmes.

« Fiction! Le projet de loi C-22 n'exigerait pas de moyens détournés. »

Vous avez répondu ceci au sujet de X: « Fait: rien dans le projet de loi C-22 n'empêcherait d'ordonner des moyens détournés, compte tenu des pouvoirs énormes conférés par les articles 5 et 7 ».

Pourriez-vous nous en dire plus à ce sujet?

David Fraser: Absolument, et je pense que c'est l'un des grands problèmes de ce projet de loi.

En ce qui concerne les intentions du projet de loi, il comporte deux parties, et elles font deux choses très différentes. L'une concerne les pouvoirs, et l'autre, les capacités.

Si vous regardez l'article 5 et la liste des choses sur lesquelles le gouverneur en conseil peut prendre des règlements, ou l'article 7 et les arrêtés ministériels, vous verrez qu'ils sont rédigés de façon extrêmement large.

Premièrement, j'attire votre attention sur les règlements que le gouverneur en conseil peut prendre. Ils comprennent tout ce qui se trouve aux alinéas 5(2)a) à 5(2)d), ce qui signifie plus que l'octroi implicite d'un pouvoir. L'alinéa 5(2)a) pourrait inclure des moyens détournés, et l'alinéa 5(2)b) pourrait inclure des moyens détournés, parce qu'ils peuvent exiger l'installation d'appareils sur l'infrastructure des FSE. Rien d'autre dans le projet de loi n'empêche cela de se produire, à part la bonne volonté du ministre et du commissaire au renseignement, et c'est tout.

Je suis particulièrement préoccupé par ces décrets secrets, parce que le ministre a le pouvoir de faire tout ce qui pourrait figurer dans un règlement public à l'égard de toute entreprise de télécommunications ou de tout fournisseur de services électroniques. Au moins, les règlements seront publiés et soumis à un processus, et les gens pourront les consulter. Cependant, les décrets secrets peuvent inclure des moyens détournés, car cela n'est certainement pas exclu dans la définition de « vulnérabilité systémique », et ils ne protègent pas le chiffrement de manière significative.

Si vous combinez ces deux éléments, les garde-fous ne sont tout simplement pas là. Le seul garde-fou est la Charte des droits et libertés, pour laquelle nous devrons intenter des poursuites afin de... Je crains que le gouvernement ne se dirige vers un échec s'il adopte un projet de loi qui va trop loin, un projet de loi qui viole la Charte et qui va être jugé inconstitutionnel. Il est préférable de bien faire les choses.

Rhonda Kirkland: Merci. Nous avons parlé à quelques reprises de bien faire les choses avec ce projet de loi, plutôt que de nous dépêcher de le faire adopter.

En ce qui concerne l'intention par rapport à ce qui est permis, si le gouvernement n'a vraiment pas l'intention de forcer des moyens détournés ou d'affaiblir le chiffrement, pouvez-vous penser à une raison de ne pas interdire clairement et explicitement ces activités dans la loi elle-même?

David Fraser: Je ne vois pas pourquoi nous ne devrions pas inclure ces garde-fous. Les garde-fous sont absolument essentiels.

Une partie de la réalité, c'est que l'intention n'a pas vraiment d'importance aujourd'hui, parce que ce qui va devenir loi, c'est ce qui est écrit dans cette loi. Le ministre va changer à un moment donné et le gouvernement va changer à un autre moment, et nous pouvons voir des changements importants au sud de notre frontière. Si ces pouvoirs existent dans un environnement politique complètement différent, ils peuvent absolument être utilisés contre les citoyens.

Il y a une expression, « totalitarisme clé en main », qui me préoccupe un peu.

Rhonda Kirkland: Merci beaucoup. Je vous en suis reconnaissante.

Monsieur Geist, dans votre article de mai 2026 intitulé « Cécité délibérée? » — avec un point d'interrogation —, vous soutenez que l'énoncé concernant la Charte que le ministère de la Justice exige du ministre de la Justice a largement ignoré certaines des dispositions du projet de loi C-22 qui sont les plus vulnérables sur le plan constitutionnel.

À votre avis, pourquoi le gouvernement a-t-il évité d'aborder de manière significative les articles du projet de loi qui sont les plus susceptibles de soulever de graves préoccupations en matière de Charte et de protection de la vie privée?

Michael Geist: Je n'ai pas de bonne réponse pour expliquer pourquoi il l'a fait ou pourquoi il n'a pas abordé ces questions, mais je dirais que je pense que cela soulève de réelles préoccupations.

Si c'est parce que le gouvernement ne croit pas que les questions relatives, disons, à la conservation obligatoire des métadonnées soulèvent des questions relatives à la Charte, et qu'il a donc estimé qu'il n'était pas nécessaire de les inclure, je pense que c'est à la fois inexact sur le plan juridique et que cela laisse également entendre, comme nous l'avons dit, que ce projet de loi sera rapidement contesté. Je pense qu'il y a un risque réel que de telles dispositions soient invalidées.

● (1720)

Rhonda Kirkland: Merci.

Le vice-président (Frank Caputo): Merci, monsieur Geist.

Nous passons maintenant à M. Zuberi, pour cinq minutes, s'il vous plaît.

Sameer Zuberi (Pierrefonds—Dollard, Lib.): Merci, monsieur le président.

Je remercie les témoins d'être ici aujourd'hui pour discuter de cet important projet de loi.

J'aimerais commencer par M. Geist.

Vous avez répondu à une question d'une collègue parlementaire, Mme DeBellefeuille, au sujet de la protection de la vie privée et de la façon dont les autres pays du Groupe des cinq et les pays européens traitent cette question.

Je suis également curieux au sujet de la surveillance judiciaire et de la façon dont le Groupe des cinq et les pays européens abordent la surveillance judiciaire dans le cadre d'une analyse comparative du projet de loi C-22.

Michael Geist: C'est une bonne question. Franchement, je n'ai pas de réponse complète à vous donner en ce qui concerne les ordonnances de communication ou les renseignements sur les abonnés sur lesquels nous nous sommes concentrés. Peut-être que l'un de mes collègues ici présents le sait.

Je m'intéresse principalement à ce qui se passe dans l'environnement des réseaux, à l'intersection entre les fournisseurs et la protection de la vie privée, et c'est là que j'ai l'impression que nous sommes en décalage.

Sameer Zuberi: D'accord. Quelqu'un d'autre a-t-il un commentaire à faire à ce sujet? Sinon, je vais poser ma prochaine question.

Nous savons qu'il y a eu des répercussions disproportionnées dans les services de police en ce qui concerne les communautés racisées, les Autochtones et différents mouvements sociaux. Craignez-vous que les répercussions de ce projet de loi soient différentes pour certaines communautés au Canada?

Michael Geist: Je peux commencer, et les autres témoins pourront peut-être poursuivre.

J'ai des préoccupations, des préoccupations que nous avons exprimées. Nous courons le risque de miner la confiance — j'en ai parlé vers la fin de ma déclaration — entre le public, ses fournisseurs et, franchement, les forces de l'ordre elles-mêmes.

Concernant les communautés où une partie de cette confiance a peut-être été, même maintenant, mise à rude épreuve, l'idée que nous créons des cadres qui réduisent les garanties qui existent en ce qui concerne la norme pour pouvoir obtenir des renseignements, et même la connaissance de base que, à mesure que les gens deviennent plus conscients des répercussions de certaines de ces dispositions, avec qui ils parlent sur leurs appareils, où ils vont et comment ils interagissent, toutes ces informations étant recueillies et conservées pendant un an, je ne pense pas que le fait de savoir que leurs fournisseurs ont ces informations augmente le niveau de confiance que les gens ont envers leurs fournisseurs. Vous ajoutez également à cela le fait que les fournisseurs ont été obligés de recueillir cette information et d'ensuite envelopper dans le secret ce qui pourrait se passer avec certaines de ces données. Je pense que tout cela mine la confiance qui existe entre le public et les différents types d'autorités avec lesquelles nous voulons augmenter le niveau de confiance.

Sameer Zuberi: D'accord. À un moment donné, vous avez parlé de gels rapides et ciblés, au lieu de l'approche actuelle. Avez-vous quelque chose à dire à ce sujet? Voulez-vous nous en dire un peu plus?

Michael Geist: Bien sûr. La notion de base entre un gel rapide, qui est, dans l'ensemble, ce qui se passe aujourd'hui, est... Nous devrions probablement revenir en arrière pour souligner qu'il n'y a aucune raison commercialement viable pour que les fournisseurs conservent des métadonnées pendant de longues périodes. Il y a des risques. Nous avons parlé de ces risques. Si l'on crée cette grosse botte de foin, pour ainsi dire, on crée une cible mûre pour les pirates informatiques ou d'autres personnes qui pourraient chercher à y avoir accès. C'est potentiellement un trésor d'information, mais au-delà de cela, c'est coûteux, ce qui peut rendre certains fournisseurs moins concurrentiels et ce qui augmente les prix auxquels les Canadiens font face pour leurs services de communication, de sorte que dans l'ensemble, ils ne le font pas.

Ce qu'ils font, cependant, c'est de créer un scénario dans lequel ils répondront à des ordonnances exigeant qu'ils conservent ces renseignements pendant qu'une enquête est en cours.

Voici ce que j'avais proposé: ne pouvons-nous pas trouver un moyen d'intégrer ce système, qui nous permet de conserver ces données en permanence, à un système qui, pendant une très courte période, au besoin, permet de les conserver et qui est ensuite rapidement éliminé? On pourrait le faire dans cette très petite minorité de situations où il faut conserver les métadonnées pendant une longue période, mais seulement si une enquête est en cours, et pas contre tous les Canadiens.

● (1725)

Sameer Zuberi: Dans les 30 secondes qui restent, est-ce que d'autres pays européens et du Groupe des cinq utilisent l'approche que vous décrivez?

Michael Geist: Le gel rapide est l'approche courante que nous observons dans les administrations qui ne conservent pas de métadonnées obligatoires. Ce n'est pas comme si les forces de l'ordre ne pouvaient pas obtenir de métadonnées ailleurs. Elles le peuvent, mais avec une surveillance appropriée, en utilisant ce modèle de gel rapide.

Le vice-président (Frank Caputo): Merci beaucoup.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour deux minutes et demie.

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur Geist, je reprends ma question de tantôt.

Le projet de loi ne comprend pas de définition claire de ce qu'on entend par « fournisseur de services électroniques ».

Pensez-vous qu'on devrait préciser davantage ce qui devrait être inclus ou exclu dans la définition du fournisseur de services électroniques ou dans celle du fournisseur de services principal?

[*Traduction*]

Michael Geist: Oui. Je sais que M. Fraser a abordé ce sujet, et il pourrait peut-être expliquer plus en détail pourquoi cette définition très large englobe bien plus que ce que la plupart des gens ne réalisent, compte tenu de son ampleur.

Je voulais revenir sur votre question à laquelle je n'ai pas eu l'occasion de répondre pleinement, à savoir: pourquoi une définition aussi large? Je crois sincèrement — et je le dis avec tout le respect que je vous dois — qu'en repensant aux nombreuses années de débat sur l'accès légal, on constate invariablement que les forces de l'ordre cherchent à obtenir le plus de pouvoirs possible, et on peut comprendre pourquoi. Elles souhaitent s'assurer de pouvoir faire leur travail aussi efficacement que possible. Cependant, ce n'est pas parce que l'on peut réclamer une approche aussi large que le gouvernement en place doive y consentir, et le Parlement ne devrait certainement pas le faire, une fois qu'il a eu l'occasion d'étudier les répercussions et les compromis qui en découlent.

Nous l'avons vu, franchement, dans le projet de loi C-2, où il y avait un excès évident de zèle en ce qui concerne l'accès sans mandat aux informations de toute personne fournissant un service au Canada. Les gens ont dit: « Attendez un instant, cela va trop loin. » Heureusement, le gouvernement a écouté les arguments avancés sur ce point, mais il reste d'autres questions où je pense que nous devons reconnaître que cela va vraiment trop loin et que nous devons revoir nos ambitions à la baisse, tout en sachant que nous répondrons quand même à bon nombre des préoccupations et des besoins des forces de l'ordre.

[*Français*]

Claude DeBellefeuille: Vous seriez peut-être d'accord pour proposer une façon de restreindre le pouvoir réglementaire qui est donné au gouvernement par cette définition. Le seul moyen de le faire serait de préciser ce qui est exclu.

N'est-ce pas?

[*Traduction*]

Michael Geist: Je pense que, pour commencer, cette notion de personnes utilisant l'information ou les services d'information de cette manière, comme l'a fait remarquer David Fraser, englobe vraiment tout le monde.

Si ce dont nous parlons vraiment, c'est que vous avez... et que la vision est... C'est difficile, car ce ne sont que des spéculations. Si ce sont simplement les grandes entreprises de télécommunications qui constituent les principaux fournisseurs, mais que nous pensons à d'autres qui offrent ce qui pourrait être considéré comme des types de services parallèles, c'est ce que j'aurais imaginé qu'un fournisseur de services électroniques pourrait être, mais ce n'est pas ce que nous avons dans la définition actuelle.

Le vice-président (Frank Caputo): Merci beaucoup, professeur Geist et madame DeBellefeuille.

Nous passons maintenant à M. Baber, pour cinq minutes, s'il vous plaît.

Roman Baber (York-Centre, PCC): Monsieur Fraser, vous êtes avocat en règle auprès du Barreau de la Nouvelle-Écosse

David Fraser: Oui.

Roman Baber: Vous exercez depuis plus de 25 ans.

David Fraser: Depuis le mois dernier, oui.

Roman Baber: Vous êtes avocat spécialisé dans les technologies et le cyberespace au sein du cabinet McInnes.

David Fraser: C'est exact.

Roman Baber: Je crois également comprendre que vous êtes un conférencier de renom sur les questions liées aux technologies et à Internet. Je suis tombé sur l'une de vos vidéos YouTube concernant ce projet de loi que nous étudions actuellement, le projet de loi C-22, sur l'accès légal, et j'aimerais fournir au Comité une brève transcription de vos propos:

« Si le projet de loi C-22, la Loi de 2026 concernant l'accès légal, est adopté, le gouvernement du Canada pourra ordonner secrètement à Apple d'intégrer à son infrastructure une fonctionnalité permettant aux forces de l'ordre et aux responsables de la sécurité nationale canadiens de suivre en temps réel chaque iPhone, chaque iPad, chaque Apple Watch, chaque AirPod d'Apple et chaque AirTag. Ils pourront alors exiger d'Apple qu'elle confirme si elle vous fournit des services.

Les forces de l'ordre pourront alors s'adresser à un juge de paix et obtenir une ordonnance, sans même avoir de raison de croire qu'un crime a été ou sera commis, exigeant qu'Apple leur remette tous les identifiants de chaque appareil que vous utilisez avec ses services. Il s'agit de l'identifiant numérique de votre iPhone, iPad, Apple Watch, AirPod, Apple TV et AirTag. Grâce à ces informations, elles pourront retourner voir le juge et obtenir une ordonnance, là encore sans avoir la moindre certitude qu'un crime ait été commis ou est sur le point d'être commis, exigeant...

Frank Caputo: Monsieur Baber, pourriez-vous ralentir un tout petit peu?

Roman Baber: J'ai presque fini.

« ... obligeant Apple à leur communiquer la localisation en temps réel de tous vos appareils. Oh, et cette ordonnance secrète obligeait également Apple à conserver l'historique de vos déplacements pendant une année entière, afin que les policiers puissent y avoir accès eux aussi. »

Quel est le problème, monsieur Fraser?

Des voix: Oh, oh!

David Fraser: Tout ça.

Certes, le contrôle judiciaire ne me pose guère de problème. Le seuil est évidemment important.

Cependant, si vous examinez l'ensemble de ces éléments dans leur globalité, la partie 2 peut exiger d'un fournisseur de services électroniques — il est indéniable qu'Apple est un fournisseur de services électroniques —, soumis à une ordonnance secrète, qu'il conserve les métadonnées, les informations de localisation, tout ce genre de choses, et même qu'il intègre de nouvelles fonctionnalités à ses appareils. C'est ce que prévoient les alinéas (2)a) et b) de l'article 7.

Une fois ces informations disponibles, il est possible de s'adresser à un juge pour obtenir une ordonnance sur la base d'un soupçon raisonnable concernant la confirmation de la notification, puis d'un soupçon raisonnable concernant les informations de base sur l'abonné, puis d'un soupçon raisonnable afin d'obtenir les métadonnées et les informations de transaction que le fournisseur a été contraint de conserver.

Il s'agit potentiellement d'un ensemble complet que nous devons examiner de manière globale et détaillée.

● (1730)

Roman Baber: Et c'est sans même croire qu'un crime a été commis, sans prêter serment dans un affidavit en disant: « Je crois qu'un crime a été commis, et par conséquent, Votre Honneur, j'obtiens une ordonnance judiciaire. »

Je voudrais réfuter certains des arguments juridiques avancés par les libéraux. Je voudrais être plus précis, si vous me le permettez, à l'égard de M. Diab.

L'un des arguments avancés au sujet de l'article 8, qui concerne la saisie arbitraire... Ce que le gouvernement propose de faire, c'est de saisir les métadonnées, dans leur intégralité, et d'ordonner qu'elles soient conservées pendant 365 jours, sans savoir ni suggérer qu'une infraction a été commise. Cependant, il existe une jurisprudence relative à l'article 8 — perquisitions et saisies arbitraires — qui suggère que la « saisie » nécessite une production. Ici, il n'y a pas de production.

Que répondez-vous à cela?

Robert Diab: La saisie réside dans la conservation des données.

Roman Baber: Exactement.

Robert Diab: Elle réside dans l'enregistrement.

Roman Baber: La saisie réside dans le fait que les informations sont conservées. Le fait qu'elles ne soient pas détenues par la police, mais conservées pour le compte de la police sur ordre du gouvernement est ce qui en fait une saisie, car c'est le gouvernement qui oblige le secteur privé à conserver ces informations.

Passons au professeur Geist. Je suis très heureux de vous voir en dehors de votre personnage Twitter.

Professeur Geist, j'ai une préoccupation majeure, notamment concernant le libellé qui précise qui peut être soumis à ces ordonnances. Plus précisément, ce sont les fournisseurs de services électroniques qui peuvent être contraints par un ministre de concevoir un système, une porte dérobée, etc. J'ai examiné la définition de « fournisseur de services » — elle figure à l'article 2, « Définitions » — et elle désigne essentiellement toute personne qui fournit des services électroniques à des personnes au Canada et qui exerce ses activités au Canada. J'ai ensuite cherché la définition de « service électronique », qui désigne tout ce qui « implique la création, l'enregistrement, le stockage, le traitement, la transmission, la réception [ou] la diffusion » de communications électroniques.

Eh bien, il me semble que n'importe quel cabinet d'avocats enverrait ou recevrait des courriels via son serveur, tout comme n'importe quelle banque ou n'importe quel cabinet médical. Les députés libéraux nous disent que seuls les fournisseurs de services Internet sont visés par cette mesure, mais ce n'est pas ce que dit le texte de loi.

Michael Geist: Cela rejoint la question soulevée plus tôt, et non, ce n'est manifestement pas ce qu'il dit pour l'instant. Son champ d'application est évidemment beaucoup plus large.

Si vous me le permettez, vous avez demandé...

Le vice-président (Frank Caputo): Je suis désolé. Vous étiez sur le point de nous livrer une idée brillante, monsieur Geist, mais nous devons à présent céder la parole à Mme Dandurand, si elle le souhaite.

Madame Dandurand, allez-y pour un maximum de cinq minutes, je vous prie.

Marianne Dandurand (Compton—Stanstead, Lib.): Oui, j'aimerais bien moi aussi entendre les idées brillantes de M. Geist.

Le vice-président (Frank Caputo): Très bien, nous allons pouvoir écouter ensemble les idées géniales de M. Geist.

Michael Geist: Eh bien, j'ai l'impression que vous m'accordez beaucoup trop de crédit.

Des voix: Ha, ha!

J'allais dire ceci: vous avez posé une question accompagnée d'une longue liste concernant Apple, en demandant en substance, quel est le problème? Le problème, bien entendu, concerne toutes ces données qui pourraient finir par être conservées et auxquelles on pourrait éventuellement avoir accès.

J'observe également un autre problème. L'imposition de certaines de ces règles risque d'amener les grandes entreprises technologiques soit à supprimer certains de leurs services de protection aux Canadiens — nous l'avons constaté avec Apple au Royaume-Uni —, soit à se retirer complètement du marché si elles ne parviennent pas à respecter les normes qu'elles s'imposent à elles-mêmes, et que leurs clients attendent en matière de protection de la vie privée. Lorsque l'on associe une définition très large du concept de « fournisseur de services électroniques » à des exigences très vagues qui peuvent être incompatibles avec la situation d'une entreprise, on crée un environnement dans lequel le Canada risque d'être marginalisé. Les entreprises concernées pourraient cesser d'offrir certains types de protections, voire cesser tout simplement de fournir leurs services aux Canadiens.

[*Français*]

Marianne Dandurand: Merci beaucoup.

Je vais laisser mon collègue M. Zuberi vous poser de brillantes questions.

[*Traduction*]

Sameer Zuberi: J'aimerais simplement demander à M. Diab et à M. Geist s'ils ont quelque chose à ajouter sur le sujet.

Robert Diab: Oui. J'aimerais faire part d'une réflexion concernant le scénario extrême qui a été avancé à plusieurs reprises pour justifier le pouvoir d'accorder au gouvernement des pouvoirs de rétention des métadonnées: l'enlèvement, la séquestration et l'exploitation sexuelle d'une jeune fille de 14 ans.

Je vois dans ce scénario une tentative de ressasser le bon vieux scénario de la « bombe à retardement » d'il y a 20 ans. À l'époque, des parlementaires avaient avancé ce scénario extrême pour justifier l'usage de la torture. Je veux rester prudent sur ce point, mais cette tactique consistait à instrumentaliser une situation extrême pour justifier et normaliser certains pouvoirs qui, autrement, seraient considérés comme inconcevables.

J'invite les membres du Comité à se demander si on tente de nous refaire le coup de la « bombe à retardement ». N'est-on pas en train de présenter un scénario particulièrement horrible, mais extrêmement rare, afin de pousser les Canadiens à renoncer à une part importante de leur liberté, de leur sécurité, et de leur vie privée? Tout cela pour permettre aux forces de l'ordre d'être un peu plus efficaces si une situation hautement improbable devait survenir.

● (1735)

Sameer Zuberi: Je vous remercie, monsieur Diab, et je vais continuer dans cette voie. Si vous ne souhaitez pas donner votre avis, ce n'est pas grave.

À l'heure actuelle, les Canadiens sont en droit de s'attendre à ce que leurs conversations privées demeurent bel et bien privées. Le simple fait qu'elle ait lieu en fait une conversation d'ordre privé.

Pourriez-vous nous expliquer en quoi les Canadiens devront inévitablement réévaluer leurs attentes en matière de vie privée si le projet de loi C-22 devait être adopté?

Robert Diab: Lorsqu'une loi est contestée et qu'un tribunal se fait demander si cela permet des fouilles, des perquisitions et des saisies raisonnables... Ce n'est pas ainsi que nos tribunaux abordent la question. Les juges prennent du recul et se posent une question du genre: « Lorsque deux citoyens canadiens communiquent dans un restaurant, par exemple, penseraient-ils qu'il est raisonnable de supposer que leur conversation est privée? S'ils s'envoient des textos, les citoyens canadiens raisonnables présument-ils que leurs textos vont demeurer privés? » Bref, c'est de cette manière que les juges réfléchissent à ce genre d'enjeux.

Lorsque le projet de loi C-22 sera éventuellement porté devant la Cour suprême du Canada, la question sera la suivante: « Le Canadien ordinaire et raisonnable suppose-t-il que le registre de ses messages au cours de la dernière année, ou le registre de ses déplacements, demeurent privés? » En ce sens qu'ils n'ont pas été enregistrés par l'État à des fins d'application de la loi, en raison de la possibilité que ces Canadiens aléatoires aient pu commettre un crime. Posez-vous la question. Si vous étiez juge, penseriez-vous que c'est exagéré, ou diriez-vous: « Bien entendu, nous ne voulons pas que nos déplacements soient enregistrés. »

Sameer Zuberi: En ce qui concerne la collecte et la rétention de métadonnées, de nombreuses préoccupations ont été soulevées au sujet des risques posés par des acteurs malveillants.

Souhaitez-vous faire part de vos inquiétudes concernant le fait que des individus auxquels nous ne souhaitons pas communiquer des renseignements puissent tout de même y avoir accès, que ce soit par l'intermédiaire des entreprises concernées ou d'acteurs malveillants, qu'il s'agisse d'États étrangers, de pirates informatiques, et ainsi de suite?

Le vice-président (Frank Caputo): Veuillez répondre très brièvement, s'il vous plaît.

Michael Geist: Je vais répondre ainsi. Je me suis présenté hier devant un comité sénatorial sur l'IA, où l'accent a été mis en grande partie sur la cybersécurité. Honnêtement, je trouve cela tout simplement ahurissant de passer d'un comité où l'on aborde des sujets tels que Claude Mythos et la nécessité absolue de renforcer la cybersécurité, à un autre comité où l'on discute d'un projet de loi visant à saper sciemment les fondements de la cybersécurité.

À mon avis, le bon sens doit...

Le vice-président (Frank Caputo): Merci beaucoup, monsieur Geist. Je suis désolé, mais le temps presse.

Je souhaite à présent faire usage de ma prérogative de vice-président, car il y a un élément dont nous allons certainement entendre parler lors de la prochaine série de questions, et qui me semble particulièrement important. Monsieur Geist, je vous demanderai de répondre très brièvement, en 15 secondes.

Vous avez mentionné qu'un délai de 30 jours pour la rétention des métadonnées serait adéquat. Souvent, il n'y a même pas un enquêteur affecté à un cas de leurre par Internet en 30 jours. En gardant cela à l'esprit, croyez-vous qu'il serait approprié d'accorder un délai de 90 jours pour la rétention des métadonnées afin de mieux traiter ce type de crimes?

Michael Geist: Je pense que la meilleure manière de répondre à votre question est de rappeler qu'une trop grande partie de l'élaboration des politiques relatives à l'accès légal ne s'est pas appuyée sur des données factuelles, mais repose plutôt sur une simple série d'anecdotes.

Il me semble que si l'on cherche à déterminer quelle est la durée appropriée — une année, c'est clairement beaucoup trop long —, il nous faut, pour être franc, bien davantage d'éléments permettant de savoir dans quels cas ces métadonnées sont réellement nécessaires, et combien de temps il faut aux forces de l'ordre pour obtenir un mandat.

Le vice-président (Frank Caputo): Très bien, nous allons essayer de revenir à ce sujet avec nos prochains invités. Merci beaucoup.

Merci à tous nos témoins.

Nous allons suspendre brièvement la séance.

● (1740)

(Pause)

● (1745)

Le vice-président (Frank Caputo): Nous passons maintenant à notre troisième groupe de témoins.

Je souhaite la bienvenue à notre prochain groupe d'invités. Nous avons le plaisir d'accueillir Monique St. Germain, du Centre canadien de protection de l'enfance; David Pierce, de la Chambre de commerce du Canada; et Mary Beth Moellenkamp, de la Société d'aide à l'enfance de Peel.

Merci à tous pour votre présence parmi nous aujourd'hui. Vous disposez de cinq minutes chacun pour faire une déclaration préliminaire.

Madame St. Germain, nous allons commencer par vous, s'il vous plaît. Merci.

Monique St. Germain (avocate générale, Centre canadien de protection de l'enfance): Monsieur le vice-président, mesdames et messieurs les députés, je tiens à vous remercier de nous avoir invités à participer à cette étude.

Je m'appelle Monique St. Germain, et je suis avocate générale au Centre canadien de protection de l'enfance, un organisme de bienfaisance qui œuvre à l'échelle nationale et internationale pour réduire le nombre de cas d'enfants disparus et victimes d'exploitation sexuelle.

Nous sommes également responsables de Cyberaide.ca, une ligne d'assistance canadienne qui permet de signaler des cas d'exploitation sexuelle d'enfants sur Internet. En 2025 seulement, nous avons reçu 28 000 signalements.

Nous assurons également la gestion du projet Arachnid, une plateforme qui se consacre en priorité au retrait de contenus liés à la pornographie juvénile. À ce jour, le projet Arachnid a émis 141 millions de notifications demandant le retrait de ce type de contenu.

Au quotidien, notre agence est directement témoin de cas flagrants d'atteinte à la vie privée d'enfants, et de matériel pédopornographique qui circule en ligne, à la vue de tous. Nous recevons directement des témoignages d'enfants et de familles touchés par des crimes en ligne tels que la diffusion de matériel pédopornographique, le leurre d'enfants en ligne, et l'extorsion. Nous saluons les mesures prévues dans le projet de loi C-22, en particulier la confirmation de la demande de service et l'ordonnance de production des renseignements sur les abonnés.

Cela fait plus d'une décennie que l'arrêt Spencer a laissé au Parlement la possibilité d'adopter une loi raisonnable. Nous espérons que cette fois-ci, nous y parviendrons enfin. Au cours de ces années, nous avons assisté à l'émergence d'un certain nombre de menaces croissantes pour les enfants, notamment une augmentation exponentielle du matériel pédopornographique en ligne. Les données publiées par Statistique Canada indiquent que les incidents liés au matériel pédopornographique ont quadruplé entre 2014 et 2024. À cela s'ajoute le leurre d'enfants en ligne: les signalements à Cyberaide.ca ont bondi de 344 % entre 2020 et 2025. Toujours selon Statistique Canada, ce type d'acte criminel a augmenté de 65 % en 2024 par rapport à 2023. L'extorsion sexuelle représente un autre fléau majeur; par exemple, Cyberaide.ca a reçu plus de 14 000 signalements depuis 2020.

Même si le nombre d'actes criminels commis contre les enfants a atteint des sommets, les données de Statistique Canada révèlent qu'en 2024, des accusations ont été portées ou recommandées dans seulement 24 % de l'ensemble des infractions sexuelles commises contre des enfants en ligne et dans seulement 6 % des cas de matériel pédopornographique. Nous devons nous demander pourquoi.

C'est évidemment complexe, mais il faut reconnaître que les délinquants ont de plus en plus souvent recours à des outils sophistiqués tels que les téléphones jetables, les serveurs de type « bullet-proof », et les VPN, ainsi qu'à des réseaux comme Tor qui masquent les adresses IP. Certaines applications sont ouvertement et délibérément conçues pour garantir l'anonymat. Les auteurs d'infractions sont capables de changer rapidement d'identité numérique grâce à de faux comptes. Il est très courant que les délinquants sexuels utilisent différents types d'applications, d'appareils, et de comptes. Par conséquent, démêler tout cet enchevêtrement s'avère une tâche particulièrement compliquée. Par ailleurs, certaines de ces enquêtes impliquent plusieurs juridictions et fournisseurs de services. La tenue des registres et la coopération entre ces fournisseurs varient considérablement, et cela ne peut manquer d'avoir un impact significatif.

Au sein de notre organisme, nous en sommes aujourd'hui à un point où près d'un tiers des contacts reçus par Cyberaide.ca ou nos autres services d'aide proviennent directement d'enfants en quête d'aide. Il ne s'agit là que des enfants qui se tournent vers nous, souvent uniquement lorsqu'ils sont en situation de crise et, dans certains cas, ont des pensées suicidaires. Au moment où ces enfants se sentent enfin capables de demander de l'aide, les preuves susceptibles d'aider la police à identifier leurs agresseurs peuvent avoir disparu. Même un seul délinquant laissé en liberté peut causer d'énormes dommages. En voici un exemple parmi d'autres: un délinquant sexuel en l'Alberta est parvenu à leurrer 92 enfants en se faisant passer pour une adolescente.

Nous souhaitons aborder un aspect précis du projet de loi C-22 que nous aimerions voir modifier. Nous estimons que la demande de confirmation de service devrait inclure des renseignements de base sur la juridiction, telles que la province et la municipalité. Il est essentiel de disposer de ce type de renseignements, en particulier au début d'une enquête, lorsque les renseignements disponibles sont limités. Connaître la juridiction permettra de s'assurer que les services de police compétents sont impliqués et que les ordonnances de production sont présentées au bon tribunal, ce qui peut aider les forces de l'ordre à mener ses enquêtes de manière beaucoup plus efficace.

Pour conclure, les enfants canadiens ont dû payer un prix très lourd pendant que ce débat fait rage. Les tentatives passées, qui ont échoué, de réforme de l'accès légal nous rappellent avec force depuis combien de temps les enfants et les familles attendent que des mesures concrètes soient prises. Nous voulons que nos forces de l'ordre puissent agir, et nous devons pour cela leur donner tous les outils nécessaires.

Merci pour votre attention.

● (1750)

Le vice-président (Frank Caputo): Je vous remercie.

Monsieur Pierce, à vous la parole pour un maximum de cinq minutes, je vous prie.

David Pierce (vice-président, Relations gouvernementales, Chambre de commerce du Canada): Je tiens d'abord à vous remercier de me donner l'occasion de m'exprimer aujourd'hui au sujet du projet de loi C-22, Loi concernant l'accès légal.

Je suis ici au nom de la Chambre de commerce du Canada, laquelle représente nos 400 chambres de commerce partenaires et nos 200 000 membres à travers le pays, ainsi que plus de 100 associations professionnelles. Je suis également ici en tant que père. Je peux vous dire que de nombreux représentants des entreprises numériques canadiennes ont eux aussi une famille. Nous voulons tous nous assurer que les forces de l'ordre puissent disposer de tous les outils nécessaires pour poursuivre les criminels, et notamment sur Internet.

Par ailleurs, je tiens à exprimer notre gratitude envers le ministre de la Sécurité publique, le ministre de la Justice, ainsi qu'à leurs équipes pour les nombreux échanges que nous avons eus au cours de l'année écoulée. Les modifications apportées au projet de loi C-22 dans la partie 1 ont répondu à de nombreuses préoccupations du secteur, et nous remercions le gouvernement d'avoir agi, mais lorsque l'on compare la partie 15 du projet de loi C-2 et la partie 2 du projet de loi C-22, il est clair que le gouvernement ne partage pas les mêmes préoccupations que la grande majorité de nos membres à la Chambre de commerce du Canada.

J'ai travaillé dans le domaine de la cybersécurité pendant des années. Je ne comprends pas pourquoi nous traitons la cybersécurité différemment des autres crimes. Si une entreprise est piratée, son PDG doit présenter ses excuses. La responsabilité incombe à l'entreprise, même si les pirates informatiques sont soutenus par un État, mais nos discussions d'aujourd'hui ne portent pas sur la manière dont nous pouvons aider les entreprises à mieux protéger leurs systèmes et nos données. Au lieu de cela, nous parlons de les obliger à installer des dispositifs, à ouvrir leurs portes numériques et à donner accès à des renseignements à des « personnes autorisées » sur ordre du gouvernement, essentiellement.

● (1755)

[*Français*]

Le vice-président (Frank Caputo): Madame DeBellefeuille, voulez-vous faire un rappel au Règlement?

Claude DeBellefeuille: L'interprète n'est pas en mesure de faire son travail.

David Pierce: Je suis désolé.

[*Traduction*]

Le vice-président (Frank Caputo): Merci beaucoup.

Monsieur Pierce, pourriez-vous parler un peu plus lentement, s'il vous plaît? Nos interprètes ont de la difficulté à suivre votre débit.

Je rappelle à tous nos témoins et à tous les députés que lorsque nous lisons un texte, nous avons tendance à parler un peu plus vite. Je vous prie donc tous de bien vouloir en tenir compte.

Merci.

David Pierce: Bien sûr, monsieur le vice-président, je vais ralentir.

Imaginons un instant que ce projet de loi soit adopté. Dans un an ou deux, imaginez des centaines, voire des milliers d'enquêtes menées par divers services de police nationaux et ministères fédéraux sur l'ensemble de nos systèmes numériques. Qui sera responsable de gérer l'ensemble des clés de sécurité? Qui sera chargé d'appliquer les correctifs et de mettre à jour l'ensemble des systèmes pour garantir leur sécurité?

Si je devais vous transmettre un seul message aujourd'hui, ce serait celui-ci. Le milieu des affaires soutient les mandats de production de données, et nous soutenons les mandats de production de données urgents, exécutables dans les 24 heures, dans des circonstances exceptionnelles. Néanmoins, nous sommes très préoccupés par la perspective qu'une personne mandatée par le gouvernement puisse accéder sans restriction à des systèmes cryptés et sécurisés pour en extraire des renseignements.

Ce qui est également déroutant dans ce débat, c'est que j'ai eu le privilège de travailler avec certains des avocats les plus talentueux au Canada, et qu'il y a actuellement un débat pour déterminer si le projet de loi C-22, dans sa partie 2, prévoit d'exiger ou non un mandat. Il est essentiel que les pouvoirs prévus dans la partie 2 du projet de loi C-22 soient modifiés afin de clarifier ce point important, en particulier dans les paragraphes 5, 7, 14 et 20 proposés.

En ce qui concerne les métadonnées, cela entraînera des coûts considérables pour les entreprises, de l'ordre de plusieurs millions de dollars en fait, non seulement pour mettre en place toute l'infrastructure nécessaire à la rétention des données, mais également pour assurer leur gestion sécurisée, ainsi que leur mise à disposition dans un format exploitable par les forces de l'ordre. Dès lors que l'on stocke de grands volumes de données sensibles, celles-ci deviennent une cible de choix pour les acteurs malveillants.

Nous reconnaissons l'importance des ordonnances de non-divulgation, mais celles-ci devraient se limiter aux mesures autorisées par les tribunaux et liées à des risques pour la sécurité nationale ainsi qu'à des enquêtes en cours.

En outre, le projet de loi C-22 risque également de pénaliser les entreprises canadiennes prospères qui exercent leurs activités ici au Canada, mais qui sont également présentes aux États-Unis et en Europe. Si vous êtes aujourd'hui un fournisseur de services électroniques basé au Canada et que vous avez des clients aux États-Unis et en Europe, le fait de vous conformer à certaines dispositions de la partie 2 pourrait vous mettre en porte-à-faux avec les autorités chargées de l'application de la loi et les organismes de réglementation de ces juridictions. Dans un contexte où nos entreprises sont déjà confrontées à des pressions en matière de compétitivité fiscale, à l'incertitude tarifaire et au risque économique général auquel nous sommes tous confrontés, ajouter une couche supplémentaire de fardeau réglementaire aux entreprises canadiennes en ce moment précis pourrait les inciter à délocaliser leurs activités.

Enfin, en ce qui concerne la définition du terme « fournisseur principal », sans modification de cet article, cette définition particulièrement vague pourrait s'appliquer à la grande majorité des entreprises canadiennes qui utilisent des moyens de communication, ou fournissent un quelconque service électronique.

Pour conclure, le milieu des affaires a très clairement fait savoir qu'il était préoccupé par le projet de loi C-2, et en particulier par sa partie 2. Je pense que nous sommes tous convaincus que le premier ministre, le ministre de la Sécurité publique, ainsi que le ministre de la Justice sauront utiliser les mesures prévues par ce projet de loi de manière adéquate, en conformité avec ce qu'ils ont déclaré. De même, je suis certain que les fonctionnaires qui étaient présents au Comité mardi vont s'engager dans ce sens. Les fonctionnaires qui ont comparu m'ont paru des gens très honnêtes et dignes de confiance...

Le vice-président (Frank Caputo): Merci beaucoup, monsieur Pierce.

Nous passons maintenant à Mme Moellenkamp, pour cinq minutes.

Mary Beth Moellenkamp (présidente-directrice générale, Société d'aide à l'enfance de Peel): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de me donner l'occasion de comparaître. Je m'appelle Mary Beth Moellenkamp et je suis la présidente-directrice générale de la Société d'aide à l'enfance de Peel.

La Société est l'agence de protection de l'enfance mandatée pour la région de Peel, ce qui comprend les interventions à l'aéroport Pearson de Toronto. Avec nos partenaires, nous dirigeons également le carrefour nCourage, qui est le centre de services intégrés de lutte contre la traite de personnes à Peel, ainsi que le Centre d'excellence en matière d'immigration pour la protection de l'enfance, ou CWICE.

Grâce à ce travail, nous voyons une corrélation entre la traite de personnes, l'immigration, l'instabilité du logement et les mouvements transfrontaliers, d'une part, et la sécurité des enfants, d'autre part, ce qui reflète les grandes tendances provinciales et nationales. Cette expérience nous donne une perspective unique sur le projet de loi C-22.

Le projet de loi C-22 répond à un véritable défi, à savoir si les systèmes légaux peuvent agir assez rapidement pour protéger les enfants dans un environnement numérique en constante évolution. Les enfants peuvent être manipulés, isolés, menacés, déplacés et contrôlés au moyen d'outils numériques plus rapidement que les systèmes ne peuvent identifier les risques et réagir. Un accès rapide et légal aux éléments de preuve numériques peut aider à localiser un enfant, à identifier l'adulte qui lui cause du tort, à prévenir toute nouvelle exploitation et à soutenir une intervention coordonnée.

En même temps, les mesures de protection sont essentielles. L'utilisation de ces outils doit être fondée sur une autorité légale, une surveillance convenable, des seuils clairs, une protection de la vie privée et un respect des droits et de la dignité des enfants.

Le système de protection de l'enfance doit trouver un équilibre difficile, mais nécessaire. Nous avons la responsabilité de préserver les enfants contre les préjudices tout en protégeant leur vie privée, leur droit à s'exprimer et leurs libertés civiles; ces deux aspects sont tout aussi importants l'un que l'autre.

Les enfants et les jeunes pris en charge par les services de protection de l'enfance sont souvent déjà davantage en contact avec le système. Ils sont surreprésentés parmi les victimes d'exploitation sexuelle et de traite. Beaucoup ont subi des traumatismes, des abus, de la négligence, une instabilité et des liens interrompus.

Les trafiquants exploitent ces vulnérabilités. Ce qui commence par une relation peut rapidement se transformer en coercition et en contrôle. Certains jeunes sont entraînés dans d'autres formes d'exploitation criminelle, notamment le vol de voitures, la fraude, le trafic de drogue ou le recrutement d'autres jeunes. Ces enfants sont souvent manipulés, menacés et isolés.

En Ontario, comme dans d'autres administrations, la traite des personnes est reconnue comme un enjeu relevant de la protection de l'enfance. Nous avons un rôle clair à jouer pour évaluer la sécurité, soutenir les personnes qui s'occupent des enfants, collaborer avec la police et les partenaires communautaires, et protéger les enfants contre les préjudices qui se poursuivent. De plus en plus, nos efforts visent à ce que les trafiquants et les exploiteurs soient considérés comme les auteurs des préjudices, plutôt que de dire que les parents et les personnes qui s'occupent des enfants ont failli à leur devoir de protection.

Les trafiquants exploitent les failles entre les systèmes et les administrations. Ils tirent parti des retards et des plateformes numériques qui évoluent plus rapidement que nos réponses juridiques et nos services. L'âge moyen du recrutement dans la traite de personnes à des fins d'exploitation sexuelles est estimé à 13 ans.

À la Société d'aide à l'enfance de Peel, nous avons pris en charge des enfants d'à peine neuf ans. L'an dernier, notre organisme a recensé plus de 200 cas où un enfant ou un jeune était soupçonné d'être impliqué dans le trafic sexuel, et pourtant, nous savons que ce nombre est considérablement sous-estimé. Souvent, un enfant ne connaît son trafiquant que par un numéro de téléphone, un pseudonyme de médias sociaux, une application, un véhicule, un hôtel ou une adresse courriel. Ces fragments d'information sont importants. Ils peuvent faire la différence entre ne pas savoir où chercher un enfant et le localiser.

L'intérêt du projet de loi C-22 pour la protection de l'enfance est indirect, mais ces dispositions législatives sont importantes. Elles pourraient aider nos partenaires policiers à obtenir des pistes numériques légales. Les agences de protection de l'enfance, les centres de lutte contre la traite de personnes, les services d'aide aux survivants et les organismes communautaires pourront en faire des plans de sécurité, ainsi que des mesures de protection et de soutien centrées sur les survivants. Les jeunes exploités doivent être traités comme des victimes et des survivants, et non comme des délinquants.

Les informations numériques ne suffiront pas à assurer la sécurité des enfants. La sécurité nécessite des systèmes coordonnés, notamment la protection de l'enfance, la police, des soutiens dirigés par des survivantes, des services adaptés aux Autochtones et aux spécificités culturelles, une expertise en matière d'immigration, des solutions de logement et des soutiens en santé mentale. Utilisé de manière légale et avec des garanties, le projet de loi C-22 pourrait aider nos partenaires à localiser les enfants plus rapidement, à démanteler plus vite les réseaux d'exploitation et à renforcer les efforts collectifs visant à protéger les enfants et les jeunes.

Merci.

● (1800)

Le vice-président (Frank Caputo): Merci beaucoup, madame Moellenkamp.

Je tiens à remercier ce groupe de témoins.

Nous allons maintenant commencer le premier tour de six minutes.

Madame St-Germain, vous ne vous souvenez probablement pas de moi, mais je vous ai consultée lorsque j'ai rédigé le projet de loi visant à remplacer le terme « pornographie juvénile » par « matériel d'abus et d'exploitation pédosexuels ». J'ai pris connaissance de votre travail pour la première fois lorsque nous avons tous les deux assisté à la même conférence provinciale sur la stratégie du Groupe intégré de lutte contre l'exploitation des enfants, ou GILEE, de la Colombie-Britannique. Pour ceux qui ne le savent pas, la GRC de Vancouver dispose d'une unité qui enquête sur Internet et sur l'exploitation d'enfants. Des gens de toutes sortes d'organismes se sont rassemblés à la conférence. J'ai vraiment aimé vos interventions à cette occasion.

Au tour précédent, nous avons parlé du temps qu'il faut pour qu'une enquête soit lancée. J'ai moi-même intenté des poursuites dans une affaire de leurre par Internet. Beaucoup de gens ne s'en rendent pas compte, mais le logiciel d'un fournisseur de services, disons Facebook, pourrait détecter une tentative de leurrer un enfant. Ensuite, si je me souviens bien — ou du moins c'était le cas auparavant —, ces informations étaient transmises au National Center for Missing & Exploited Children de Washington, D.C. Je crois que le dossier serait ensuite transmis au quartier général national de la GRC, puis à la province. Est-ce à peu près exact?

● (1805)

Monique St-Germain: Oui, en supposant que l'information passe par le système de signalement obligatoire aux États-Unis.

Le vice-président (Frank Caputo): Oui, exactement.

Monique St-Germain: C'est ainsi que les choses se passent.

Le vice-président (Frank Caputo): Ce processus prend un certain temps. J'ai posé la question à l'un des juristes du groupe de témoins précédent. Quand on parle de conservation des données, combien de temps faut-il les garder? Je ne pense pas que quiconque estime que les données devraient être conservées indéfiniment. Vous êtes avocate. Vous comprenez le point de vue des gens. Il faut aussi voir pendant combien de temps les données doivent être conservées pour l'enquête.

D'après votre expérience, pouvez-vous nous dire combien de temps il faut pour qu'une enquête avance jusqu'au point où quelqu'un l'examine et se rende compte qu'il manque quelque chose? Par exemple, il pourrait s'agir d'une adresse IP manquante qui constitue une lacune en matière de preuve, car l'information aiderait les enquêteurs à attraper un prédateur d'enfants. J'espère que je m'exprime clairement.

Monique St-Germain: Oui, je comprends ce que vous demandez. Je ne suis pas sûre d'être la bonne personne à qui poser cette question. Nous ne sommes pas la police. Le rôle que nous jouons est très distinct et séparé de celui des corps policiers. Nous recevons des informations provenant de diverses sources et les transmettons à la police, mais c'est elle qui connaît le processus d'enquête suivi.

Nous savons, de notre point de vue dans le continuum, que souvent, lorsque les enfants et les familles canadiennes nous envoient des signalements, il est impossible d'y donner suite. Au moment où l'information parvient à la police, il se peut qu'il n'y ait pas suffisamment d'éléments pour qu'elle puisse agir. Il y a certainement eu des retards dans l'obtention des renseignements sur les abonnés permettant aux enquêteurs de relier les données dont ils disposent à un lieu précis et de pouvoir ainsi commencer à enquêter sur quelqu'un.

Par exemple, une adresse IP peut mener à une maison donnée, mais quatre personnes peuvent y vivre. C'est tout un processus. Chaque étape permet d'affiner la recherche et de se rapprocher de l'individu en question.

En ce qui concerne les métadonnées, d'après ce que je comprends du projet de loi, c'est la réglementation qui déterminera quelles métadonnées sont collectées, stockées et pendant combien de temps. Il s'agit d'un processus important permettant de clarifier quelles informations seront utiles. Il est certain, d'après ce que nous observons dans les tribunaux, que ces informations sont essentielles pour établir un lien entre un délinquant et une activité précise en ligne.

Le vice-président (Frank Caputo): Je vous en suis reconnaissant.

L'un des plus grands défis que j'ai rencontrés consistait à établir un lien entre la personne au banc des accusés et celle qui se trouvait derrière l'écran d'ordinateur ou le téléphone, car il faut disposer de preuves reliant chaque maillon de la chaîne.

Combien de temps faut-il généralement compter entre le moment où vous recevez un signalement et celui où vous pouvez transmettre des informations à un service de police?

Monique St. Germain: Notre rôle consiste à transmettre les signalements aussi rapidement que possible. Nous traitons les informations, et si elles semblent indiquer un acte criminel, nous les envoyons au service de police compétent.

Nous utilisons des outils pour essayer de trouver ce que nous pouvons, à partir des informations reçues. Nous n'obtenons pas nécessairement des adresses IP ou ce genre de données. Nous avons ce que l'enfant nous dit, comme le nom d'utilisateur de la personne ou une description de ce qui se passe. Nous essayons d'envoyer la police là où se trouve l'enfant, à moins que nous ne puissions découvrir quelque chose sur l'auteur des faits.

Nous traitons l'information assez rapidement. Dans les 48 heures, voire plus tôt, quelque chose sera fait. Nous essayons bien sûr d'établir des priorités et de tout faire très rapidement.

Le vice-président (Frank Caputo): Ce nom d'utilisateur est ensuite utilisé pour obtenir une ordonnance de communication, idéalement faite sous serment ou affirmation, ce qui est une des raisons d'être du projet de loi.

Madame Moellenkamp, avez-vous quelque chose à ajouter à ce sujet, compte tenu de votre expertise?

Mary Beth Moellenkamp: Puis-je vous demander de répéter la question?

Le vice-président (Frank Caputo): Je vous demandais simplement combien de temps il faut, selon votre expérience, pour lancer une enquête. Avez-vous une idée du délai requis? Je sais que vous n'êtes pas policière, mais j'essaie d'en avoir une idée.

Mary Beth Moellenkamp: Dans le système de protection de l'enfance, nous évaluons l'admissibilité en fonction du niveau de risque que court l'enfant. Nous pouvons déterminer qu'il faut aller voir un enfant dans les 12 heures, ou établir que le risque est plus modéré et que nous pouvons y aller dans les 7 jours. Lors d'une intervention dans les 12 heures, nous travaillons souvent en collaboration avec la police. Des règlements pris en vertu de notre loi portent sur les enquêtes conjointes.

J'ai constaté certaines difficultés à obtenir les données nécessaires pour intervenir — pour savoir où se trouve un enfant, en particulier lors d'une disparition ou d'une alerte Amber. Nous avons connu des situations où il a été difficile d'avoir ces informations. La police attend une ordonnance, mais ce n'est pas assez vite.

● (1810)

Le vice-président (Frank Caputo): Merci. Je suis désolé de vous interrompre, mais nous devons passer à M. Ramsay pour six minutes.

[*Français*]

Jacques Ramsay: Monsieur Pierce, le hasard veut que vous soyez en compagnie de deux personnes qui s'occupent de la cybercriminalité, entre autres choses.

Vous avez entendu parler, notamment, d'un accusé qui a fait 92 victimes âgées de 9 à 13 ans. On parle de plus de 200 appels par année. Il est urgent de donner aux forces de l'ordre les pouvoirs nécessaires pour être efficaces. L'approche du « blocage rapide », dans ce cas-ci, ne fonctionne pas. Comme on vous l'a dit, il y a souvent une dénonciation qui est faite plusieurs mois après que l'infraction a eu lieu.

Compte tenu de cela, comment conciliez-vous vos demandes avec les besoins, considérant tout cela?

On parle de pédocriminalité, mais on pourrait parler aussi d'extorsion visant des commerces. Récemment, à Surrey et à Brampton, il y a eu des crimes à répétition. Alors, il est urgent de donner une information complète en temps opportun. J'aimerais que vous me disiez comment vous conciliez cela avec vos demandes.

[*Traduction*]

David Pierce: Je commencerai par aborder la question sous l'angle de la cybersécurité.

Je ne pense pas que la sécurité de quiconque soit renforcée si nos systèmes sont compromis. C'est un point essentiel. Toutes vos données, mes données et celles de nos familles… Il s'agit de données financières, de photos ou de tout autre élément, y compris les données de localisation indiquant que vous n'êtes pas chez vous, ce qui permet de cambrioler votre domicile. Le monde entier est numérique. Si nous perdons le chiffrement de ces grands systèmes, un risque fondamental pèsera sur l'économie canadienne. Un risque fondamental menacera la réussite des entreprises de notre pays. Cela nous placerait dans une position désavantageuse sur la scène internationale par rapport aux pays où les systèmes des grands fournisseurs proposant ces services seraient menacés.

D'un point de vue commercial, je pense qu'il est essentiel de garder à l'esprit le contexte dans lequel nous nous trouvons actuellement. La conjoncture économique n'est pas favorable. Dans le cas des grands fournisseurs, nous parlons d'ajouter des millions de dollars de dépenses supplémentaires à leur bilan. Qu'en est-il des petites entreprises et des fournisseurs de services électroniques au pays qui comblent les lacunes laissées par les grandes? Elles n'ont pas la capacité de s'adapter et de financer des opérations à grande échelle pour, en substance, soutenir les forces de l'ordre qui viennent installer un dispositif sur leurs systèmes, et de collaborer avec elles sur une longue période à cette fin.

Je vais revenir à ma déclaration préliminaire, si vous me le permettez.

Nous voulons tous que les forces de l'ordre disposent d'outils efficaces. Nous voulons tous que les forces de l'ordre soient en mesure de poursuivre les criminels et de protéger nos enfants et nos familles — nous tous. Il est très important que les mesures prévues dans ce projet de loi trouvent un équilibre entre la protection de nos données et de notre vie privée et, par-dessus tout, la protection de nos systèmes cryptés.

Jacques Ramsay: D'accord.

[*Français*]

Le projet de loi prévoit également une interdiction pour...

[*Traduction*]

Il est interdit aux fournisseurs de services électroniques de mettre en place une fonctionnalité qui introduirait une vulnérabilité systémique. D'une certaine manière, vous estimez que ce n'est pas suffisant.

David Pierce: Je vais vous donner un exemple. J'ai regardé les témoignages de mardi. Une des fonctionnaires a dit que dans bon nombre de ces systèmes, il y a deux clés, de sorte que nous pouvons simplement demander aux fournisseurs d'émettre une troisième clé ou une autre clé que nous pourrions utiliser.

La cybersécurité n'est pas seulement une question de technologie. Elle repose à parts égales sur la technologie et les humains. Les interactions humaines avec la technologie... Je suis sûr que tout le monde connaît une personne qui a ouvert un courriel ayant introduit un virus dans son système. La question est: qui gère ces clés? Qui protège ces clés? Comment ces clés sont-elles protégées? Qui y a accès? Les clés changent. Qui met à jour ces clés? Qui installe les correctifs sur ces systèmes?

Prenez l'exemple du Centre d'analyse des opérations et déclarations financières du Canada, ou CANAFE. Prenez certains de ces grands pirates informatiques de Salt Typhoon, qui sont des acteurs très sophistiqués. C'est drôle: je reviens à ma remarque d'ouverture, où j'ai exprimé un peu de frustration, simplement parce que la cybersécurité est considérée différemment de tous les autres crimes. Les vrais pirates informatiques d'aujourd'hui ne se trouvent pas dans un sous-sol d'une de nos grandes villes. Ce sont des adversaires étrangers. Ils sont soutenus par des États. Ce sont des opérations sophistiquées. Si vous ajoutez simplement une nouvelle porte à l'arrière du système, ils y seront lundi. Si la porte apparaît mardi, ils diront: « Hum, c'est différent. Ce n'est pas comme les autres portes. » Ils commenceront à l'explorer, et elle deviendra immédiatement une cible.

Encore une fois, j'en reviens au fait que la préoccupation principale du monde des affaires porte, d'une part, sur le chiffrement et la protection de ces systèmes; mais, d'autre part, sur la garantie que nous avons la capacité de mener nos activités commerciales et que nous pouvons avoir confiance dans la sécurité de nos systèmes et de nos informations. Si les dispositions qui figurent à la partie 2 du projet de loi C-22 sont mises en œuvre comme elles sont rédigées, le libellé ne dissipe pas les préoccupations que je viens d'exposer.

● (1815)

[*Français*]

Le vice-président (Frank Caputo): Madame DeBellefeuille, vous avez la parole pour six minutes.

[*Traduction*]

Merci, monsieur Ramsay.

[*Français*]

Claude DeBellefeuille: Merci, monsieur le président.

Ma question s'adresse au représentant de la Chambre de commerce du Canada.

À une époque où les droits de douane américains créent une grande instabilité pour nos entreprises, considérez-vous que le fait de ne pas savoir quelles entreprises sont assujetties à la loi sur l'accès autorisé à l'information entraîne une incapacité de prédire l'avenir qui peut nuire aux affaires?

[*Traduction*]

David Pierce: Tout à fait. Je vais vous faire part, en toute honnêteté, de la discussion qui a eu lieu au sein du secteur lorsque cette législation a été introduite pour la première fois. Beaucoup d'entreprises pensaient qu'elles étaient exclues, simplement parce qu'elles n'étaient pas des fournisseurs de services électroniques. Cependant, quand on examine vraiment cette définition, on constate qu'il s'agit d'une personne qui fournit des services électroniques. Qu'utilisez-vous aujourd'hui qui ne fasse pas appel à une forme quelconque de communication électronique? Ma voiture en fait partie. Nous disposons d'une multitude d'appareils et d'équipements différents. Il n'est pas possible de limiter le champ d'application à un petit sous-ensemble en se basant uniquement sur le libellé de la loi.

Nous suggérons qu'un critère de fonction primaire soit appliqué à la définition de fournisseur principal, afin de restreindre le champ d'application aux entreprises qui exercent spécifiquement une activité de communication, ce qui, en fin de compte, doit être l'objectif des forces de l'ordre. Cependant, si la situation reste telle qu'elle est actuellement... Lorsque nous avons examiné cette question avec nos membres partout au pays, les industries pensaient initialement qu'elles étaient exclues. Puis elles ont réexaminé le texte et ont déclaré: « Bon sang, vous avez raison. La législation pourrait nous viser. » Nous espérons que cette ambiguïté sera vraiment levée au cours du processus.

[*Français*]

Claude DeBellefeuille: Pensez-vous que les entreprises du Québec et du Canada sont prêtes à répondre aux exigences du projet de loi C-22?

Est-ce que certains de vos membres se disent prêts? Honnêtement, monsieur Pierce, je crois que le projet de loi va probablement être adopté, même si nous espérons qu'il soit bonifié.

Considérez-vous que les efforts à faire pour vous préparer à répondre aux attentes imposées par le projet de loi C-22 sont géants? Est-ce que c'est coûteux?

Vous nous avez dit que ça avait des conséquences économiques. Est-ce que vous les avez chiffrées?

Avez-vous fait une évaluation de ce que ça allait coûter de vous conformer aux attentes et aux exigences du projet de loi?

[*Traduction*]

David Pierce: Je vais commencer par parler du coût et je répondrai ensuite au reste de la question.

Les grands fournisseurs devront investir des millions de dollars dans le dessein de se doter de l'infrastructure nécessaire pour se conformer à la mesure, et les coûts opérationnels se chiffreront aussi dans les millions. Il est très important de se rappeler que les métadonnées ne sont pas faciles à lire. Pour que les forces de l'ordre puissent s'en servir, elles doivent être converties en un format utilisable.

Le projet de loi est divisé en deux parties. Je crois que le greffier vous remettra les versions française et anglaise d'une lettre de la Chambre de commerce adressée aux membres du Comité qui indique les dispositions, dans la partie 1 et la partie 2, où nous croyons que des améliorations s'imposent. Nous comprenons l'arrêt Spencer. En ce qui concerne la partie 1, des modifications ont été apportées, et notre lettre contient des recommandations. Il faudrait peut-être envisager de scinder le projet de loi afin de faire avancer la partie 1 et de répondre aux préoccupations dont les deux autres témoins ont parlé si éloquemment. Ainsi, la partie 2 pourrait être examinée plus attentivement.

De mon point de vue, les pouvoirs prévus aux articles proposés 5, 7, 14 et 20... Beaucoup d'avocats avec qui j'ai discuté au cours de la dernière année ont déclaré qu'ils ne pouvaient pas déterminer avec certitude si un mandat est nécessaire ou non. À mes yeux, c'est un signe qu'il faut poursuivre la réflexion et continuer à retravailler le projet de loi. Je ne voudrais surtout pas que le projet de loi soit adopté afin de régler les problèmes visés par la partie 1, mais que son adoption cause ensuite une multitude de problèmes commerciaux et économiques.

● (1820)

[*Français*]

Claude DeBellefeuille: Si le gouvernement avait été majoritaire, le projet de loi C-2 aurait été adopté, malgré une opposition unanime. Le gouvernement a fait un meilleur travail pour créer le projet de loi C-22, et il a mené des consultations. Alors, sincèrement, je ne suis pas très favorable à votre suggestion de scinder le projet de loi en deux.

Auriez-vous des amendements très précis à nous communiquer qui permettraient de réduire, par exemple, les répercussions sur les entreprises, ou qui pourraient les aider à faire la transition et à se conformer aux exigences prévues dans le projet de loi C-22?

Étant donné que vous avez consulté beaucoup d'avocats, j'imagine que vous devez avoir certaines améliorations à recommander. Avez-vous des suggestions très précises?

[*Traduction*]

David Pierce: J'attendais la question avec impatience. Certes, nous serions ravis de vous proposer des amendements visant à corriger le projet de loi de façon à répondre aux préoccupations que j'ai soulevées. Plus particulièrement, vous trouverez dans la lettre que le greffier vous remettra, je présume, la liste des enjeux que nous avons cernés dans la partie 1, la partie 2 et l'ensemble du projet de loi. Bien entendu, nos recommandations seraient fondées sur ces enjeux.

Je vous remercie pour la proposition.

[*Français*]

Claude DeBellefeuille: Les délais pour l'étude du projet de loi C-22 sont assez courts et, comme membres du Comité, nous devons transmettre nos amendements d'ici le 27 mai. C'est juste pour vous dire que toutes les suggestions pour améliorer le projet de loi C-22 seront les bienvenues.

Je voudrais aussi vous remercier de parler au nom des entreprises. Nous avons une diversité de témoins, et c'est ce qui nous permet de nous faire une meilleure idée sur les améliorations à apporter au projet de loi.

Je vous remercie beaucoup, monsieur Pierce.

Le vice-président (Frank Caputo): Merci, madame DeBellefeuille.

[*Traduction*]

Pour la gouverne du Comité, je souligne que nous avons pris un peu de retard. Ce n'est pas faute d'efficacité, c'est parce que les déclarations préliminaires sont plus nombreuses que d'habitude.

Afin d'accorder suffisamment de temps au prochain groupe de témoins, je propose de donner maintenant quatre minutes au Parti conservateur, puis quatre minutes au Parti libéral. Ensuite, nous passerons au prochain groupe de témoins; ainsi, nous terminerons à l'heure prévue. J'espère que cette proposition vous convient.

Nous passons à M. Lloyd, qui dispose de quatre minutes.

Dane Lloyd: Merci aux témoins.

Bonsoir, monsieur Pierce. Je suis heureux de vous revoir après tout ce temps.

David Pierce: Bonsoir, monsieur.

Dane Lloyd: Je me demande si une définition plus précise du terme « risque systémique » apaiserait les intervenants du milieu des affaires. Est-ce que cela répondrait à certaines de leurs préoccupations?

David Pierce: Tout à fait, surtout à la lumière des témoignages de mardi. La clé, c'est que le projet de loi précise qu'il ne s'agit pas strictement d'introduire une vulnérabilité systémique et que les fournisseurs de services ne seront pas obligés de compromettre le chiffrement. C'est un principe très important qui est tenu pour acquis dans la définition actuelle, mais qui, selon nous, devrait être enchâssé explicitement dans la loi pour répondre aux préoccupations de l'industrie.

Dane Lloyd: Mme West a mentionné que ces pouvoirs devraient relever des entreprises et des fournisseurs, et non des organismes d'application de la loi. D'après vous, est-ce la solution à privilégier?

David Pierce: Je vais répéter ce que j'ai dit durant ma déclaration préliminaire.

Je crois que le milieu des affaires appuie sans réserve les dispositions relatives aux situations d'urgence et à la réduction du temps de réponse aux ordonnances de communication. Les entreprises connaissent leurs systèmes. Elles savent où se trouvent les données, comment les extraire et comment les fournir dans un format utile, tout en évitant d'introduire le genre de vulnérabilité dont nous avons parlé en termes clairs.

Dane Lloyd: Voici une de mes préoccupations. Disons qu'un agent d'application de la loi s'adresse à l'un de vos membres, un fournisseur de services, et lui dit qu'il doit accéder à son système. L'entreprise va demander un mandat ou un arrêté ministériel. Si un arrêté ministériel permet aux forces de l'ordre d'accéder directement aux systèmes, quelles mesures de protection sont en place pour veiller à ce que des acteurs malveillants n'abusent pas de cet accès?

Nous avons entendu des allégations voulant que des personnes chargées d'appliquer la loi aient fait des recherches, par exemple, sur leur ex-conjoint. Quelles garanties peuvent être ajoutées au projet de loi pour empêcher les acteurs malveillants d'utiliser cette nouvelle mine de données de manière abusive?

● (1825)

David Pierce: Il y a des acteurs malveillants et il y a des concurrents qui pratiquent l'espionnage industriel. La propriété intellectuelle de ces entreprises est extrêmement précieuse. Il est très risqué de donner un accès illimité qui permettrait à quelqu'un de consulter ces renseignements à sa guise.

Comme je l'ai déjà mentionné, nous privilégions les ordonnances de communication. Selon nous, c'est la solution la plus claire.

Dane Lloyd: Merci.

Je veux poser une brève question à Mme St. Germain.

[*Difficultés techniques*] Les centres intégrés de lutte contre l'exploitation des enfants m'ont dit que bon nombre de leurs enquêtes ont été interrompues parce qu'ils se fient principalement aux informations qu'ils reçoivent du FBI.

Le projet de loi règle-t-il les problèmes découlant de la décision prise à cinq voix contre quatre dans l'affaire Bykovets?

Monique St. Germain: Je n'ai pas entendu la première partie de votre question. Il n'y avait pas de son.

Dane Lloyd: Les centres intégrés de lutte contre l'exploitation des enfants m'ont dit que beaucoup des informations qu'ils reçoivent proviennent du FBI. Ont-ils dû interrompre leurs enquêtes à cause de l'arrêt Bykovets? Le projet de loi règle-t-il ce problème?

Monique St. Germain: Il aide à le régler.

La partie 1 comprend des dispositions sur la fourniture volontaire de renseignements; on y précise que la police peut se servir des renseignements fournis volontairement. Beaucoup d'informations qui proviennent du National Center for Missing & Exploited Children aux États-Unis sont fournies volontairement. Les informations reçues sont transmises à la police. À certains endroits, l'incertitude plane sur la question de savoir si la police peut, oui ou non, les utiliser pour ouvrir une enquête.

Oui, les dispositions de la partie 1 concernant les précisions et la fourniture volontaire aident à régler le problème.

Le vice-président (Frank Caputo): Merci.

Madame Acan, la parole est à vous pour les quatre dernières minutes.

Sima Acan: Merci beaucoup, monsieur le président.

Ma première question s'adresse à M. Pierce.

La lettre ouverte que nous avons reçue soulève le risque que les ordonnances soient utilisées pour obtenir des renseignements médicaux ou financiers confidentiels.

Pouvez-vous expliquer au Comité que le paragraphe 487.0121(3) proposé interdit explicitement de donner tout ordre qui révélerait des renseignements médicaux ou des renseignements protégés par le secret professionnel?

David Pierce: Excusez-moi, votre question concerne-t-elle la partie 1 ou la partie 2?

Sima Acan: Elle concerne la partie 1.

David Pierce: Je suis désolé, je ne connais pas l'article en question. Me permettez-vous de vous revenir là-dessus, s'il vous plaît?

Sima Acan: Je vous en prie.

Mes autres questions s'adressent au Centre canadien d'aide à l'enfance, ou CCPE, et à la SAE de Peel.

Au fil de nombreuses années, j'ai consacré d'innombrables heures à des activités bénévoles auprès d'organismes comme SAVIS of Halton. SAVIS joue un grand rôle dans ma région d'Oakville. Il occupe une place centrale au sein du groupe Halton Collaborative Against Human Trafficking, groupe qui rassemble des partenaires et des organismes communautaires afin de mettre en place une réponse régionale coordonnée pour lutter contre la traite des personnes. C'est un organisme comme les vôtres.

Les organismes comme les vôtres jouent un rôle crucial dans la protection des personnes vulnérables, dans la sensibilisation de la population et dans les efforts de prévention. Malheureusement, les trafiquants se servent souvent d'Oakville et de Burlington comme lieux de transit en raison de leur proximité avec de grands axes routiers; ils déplacent leurs victimes d'un hôtel à l'autre le long de ces routes pour éviter la détection.

Nous sommes chanceux de pouvoir compter sur les membres dévoués du Service de police régional de Halton. Je tiens à les remercier sincèrement pour le travail qu'ils accomplissent sans relâche en vue de combattre ces crimes odieux.

Au cours de la dernière année, j'ai discuté avec de nombreux responsables de différents organismes d'application de la loi. Tous ont souligné que les enquêtes liées à l'exploitation d'enfants sont extrêmement complexes et qu'elles prennent énormément de temps. Ces affaires prennent souvent plus de six mois à résoudre, notamment parce que les criminels utilisent des téléphones, des ordinateurs, des services infonuagiques et des appareils de stockage pour cacher le contenu illicite.

De votre point de vue, de quelle manière le projet de loi C-22 renforcerait-il la capacité des organismes d'application de la loi de lutter contre l'exploitation des enfants et la traite des personnes, et d'enquêter sur ces infractions?

● (1830)

Mary Beth Moellenkamp: Grâce au projet de loi C-22, les organismes d'application de la loi accéderaient plus rapidement aux renseignements. Lorsque nous enquêtons, nous n'avons parfois que quelques minutes ou quelques heures pour protéger un enfant.

Parlons de l'aéroport Pearson.

Il arrive que des enfants et des jeunes qui ont été identifiés se retrouvent à l'aéroport. Il est important d'avoir accès aux renseignements et à l'empreinte numérique parce qu'une fois que l'enfant quitte l'aéroport, il se peut qu'on ne le revoie jamais et qu'on perde sa trace.

Ce que vous avez dit est juste: dans le Grand Toronto, les voies de transport sont nombreuses, des routes aux aéroports. Cette situation présente des défis. L'accès rapide est extrêmement important parce que dans des affaires pareilles, chaque minute compte.

Sima Acan: Merci beaucoup.

Madame St. Germain, voulez-vous ajouter quelque chose?

Monique St-Germain: Je dirais que les dispositions de la partie 1 seraient particulièrement utiles parce que dans de nombreuses enquêtes concernant l'exploitation sexuelle d'enfants qui reposent sur des informations provenant du NCMEC ou de sources semblables, les renseignements sont très limités. La police ne peut pas faire grand-chose avant d'en savoir plus. L'ordre de fournir des renseignements, de pair avec...

Le vice-président (Frank Caputo): Merci, madame St. Germain. Je m'excuse, mais je dois vous interrompre. Je suis vraiment désolé. Nous accusons du retard.

Sima Acan: Cinq minutes, c'est trop court.

Le vice-président (Frank Caputo): J'encourage tous les témoins qui le souhaitent à fournir des renseignements supplémentaires au Comité. Vous jouez tous un rôle essentiel. Au nom du Comité et de la population canadienne, je vous remercie pour votre travail. Nous vous sommes très reconnaissants.

Nous allons suspendre la séance le plus brièvement possible, idéalement pendant 90 secondes.

● (1830)

_____(Pause)_____

● (1835)

Le vice-président (Frank Caputo): Reprenons.

Je vous prie d'excuser la rudesse. Je tiens à remercier tous les témoins qui se joignent à nous aujourd'hui. Nous avons d'excellents invités très distingués. Je ne veux pas perdre un seul instant avec eux.

Je vous les présente.

Nous recevons Rachel Curran et Robyn Greene, de Meta Platforms Inc. Nous accueillons aussi l'honorable Marie Deschamps, Craig Forcese et Lawrence Mangano, de l'OSSNR. Finalement, je souhaite la bienvenue à l'honorable Simon Noël et à Justin Dubois.

Nous entendrons maintenant les déclarations préliminaires.

Je dois quitter le fauteuil pendant à peu près trois minutes. Si un problème survient, Mme DeBellefeuille s'en occupera. J'espère être de retour dans trois ou quatre minutes. Sinon, je vous prie de passer à la déclaration suivante. Merci.

Nous allons commencer par la déclaration préliminaire des représentantes de Meta.

Rachel Curran (directrice des politiques publiques, Meta Platforms Inc.): Merci, monsieur le président.

Bonsoir. Nous vous remercions de nous donner l'occasion de comparaître devant le Comité aujourd'hui. Je m'appelle Rachel Curran et je suis directrice des politiques publiques pour le Canada chez Meta. Je suis accompagnée de ma collègue Robyn Greene, qui est experte en la matière à l'étude. Je vous prie de lui adresser vos questions techniques.

Meta est fermement engagée à protéger la sécurité de ses utilisateurs au Canada, tant en ligne que hors ligne. Nous coopérons régulièrement avec les organismes canadiens d'application de la loi de tous les échelons du gouvernement, notamment en signalant proactivement les menaces que nous détectons, ainsi qu'en répondant aux mises en demeure valides et aux demandes d'urgence provenant des autorités canadiennes.

Nous saluons les efforts déployés par le gouvernement en vue de répondre à bon nombre des préoccupations soulevées à l'égard de la partie 14 du projet de loi C-2. Nous sommes d'avis qu'avec des amendements ciblés, la partie 1 du projet de loi C-22 fournira aux organismes d'application de la loi un cadre juridique efficace pour obtenir les renseignements nécessaires en temps opportun. Cependant, la partie 2 est une autre paire de manches: elle risque de nuire à la sécurité de la population canadienne plutôt que de la renforcer.

D'abord, les obligations d'assistance technique prévues à la partie 2 pourraient contraindre les entreprises privées à servir de prolongement de l'appareil de surveillance de l'État. Dans sa forme actuelle, le projet de loi pourrait obliger les entreprises comme Meta à mettre en place ou à entretenir des moyens de contourner ou d'affaiblir le chiffrement, et il pourrait forcer les fournisseurs à installer des logiciels espions gouvernementaux directement dans leurs systèmes.

Ensuite, le projet de loi prétend atténuer les risques pour le chiffrement en permettant aux entreprises de contester tout ordre qui introduirait une « vulnérabilité systémique »; toutefois, la notion de « vulnérabilité systémique » n'est pas clairement définie. En outre, des termes essentiels comme « chiffrement » ne seront définis que dans la réglementation, qui pourra être contournée au moyen d'arrêtés ministériels. De plus, le projet de loi ne prévoit aucun mécanisme pour contester un ordre problématique ni de protections en matière de responsabilité pour les entreprises pendant qu'une contestation est en cours.

Le consensus du milieu de la technologie est sans équivoque: il n'est pas possible d'introduire un accès aux systèmes chiffrés réservé aux organismes d'application de la loi sans créer de vulnérabilités qui seront — je dis bien « seront », et non pas « pourraient être » — exploitées par des acteurs malveillants. L'affaiblissement du chiffrement ne touche pas seulement la cible d'une enquête; il touche l'ensemble des Canadiennes et des Canadiens qui dépendent de communications sécurisées pour effectuer des transactions bancaires, pour accéder à des soins de santé, pour gérer leur entreprise ou simplement pour parler à leur famille.

Ce risque n'est pas hypothétique. Des gouvernements partout dans le monde subissent encore les conséquences des cyberattaques parrainées par l'État chinois connues sous le nom de « Salt Typhoon », cyberattaques qui ont exploité la législation beaucoup plus étroite des États-Unis en matière d'assistance technique. Les organismes de sécurité canadiens en sont conscients: ils ont recommandé explicitement l'adoption du chiffrement comme mesure de protection contre ce type de cyberattaques.

La partie 2 du projet de loi C-22 irait dans la direction opposée; elle placerait le Canada en décalage avec ses principaux alliés. L'an dernier, la France et la Suède ont abandonné des propositions similaires, et l'Union européenne a garanti des protections robustes du chiffrement dans son accord sur la sécurité en ligne. L'utilisation d'un pouvoir comparable au Royaume-Uni, qui a ordonné à Apple de compromettre son service infonuagique chiffré, a suscité une condamnation du gouvernement américain et de 200 organisations de la société civile, et elle a fini par conduire Apple à retirer son service de protection avancée des données.

L'imposition de telles obligations freinerait aussi l'innovation et l'investissement au pays, tout en nuisant à la compétitivité du Canada à l'étranger.

Par ailleurs, la portée excessive des ordonnances de non-divulgation prévues à la partie 2 risque de miner la transparence et la confiance du public. De plus, les dispositions du projet de loi relatives à la conservation des données établiraient un cadre permettant de collecter les données de Canadiens ordinaires n'ayant aucun lien avec un acte criminel, en plus de conférer aux autorités le pouvoir de perquisitionner dans les locaux d'entreprises et de saisir des données.

Compte tenu de ces problèmes majeurs, nous exhortons les décideurs de dissocier la partie 2 du projet de loi C-22 afin d'accorder à ces enjeux cruciaux l'attention et le temps qu'ils méritent.

Pour éviter les conséquences les plus néfastes sur la protection des données et la sécurité, il faut notamment retirer toute obligation contraignant les entreprises à intégrer des outils de surveillance ou d'autres logiciels du gouvernement ou de tiers à leurs systèmes; renforcer la définition du terme « vulnérabilité systémique » afin d'exclure explicitement toute exigence qui affaiblirait ou compromettrait le chiffrement; et codifier le mécanisme permettant aux entreprises de contester les ordres.

● (1840)

Merci, monsieur le président.

Le vice-président (Frank Caputo): Merci, madame Curran. Je m'excuse, mais je dois être impitoyable avec le temps.

[*Français*]

Madame Deschamps, vous avez la parole pour cinq minutes.

L'hon. Marie Deschamps (présidente, Office de surveillance des activités en matière de sécurité nationale et de renseignement): Monsieur le président, membres du Comité, bonsoir.

Je vous remercie de nous avoir invités à prendre part à vos travaux.

Je suis la présidente de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, mieux connu sous son acronyme anglais, NSIRA. Je suis accompagnée de notre vice-président, M. Craig Forcese, et du directeur général intérimaire de notre secrétariat, M. Lawrence Mangano.

[*Traduction*]

J'aimerais employer le temps qui nous est accordé pour aborder deux points.

Compte tenu de la portée des nouveaux pouvoirs proposés dans le projet de loi, il est essentiel de mettre en place un processus d'examen indépendant qui soit prompt et efficace.

[*Français*]

C'est mon premier point.

[*Traduction*]

Deuxièmement, dans sa forme actuelle, le projet de loi ne permet pas d'instaurer un tel processus d'examen.

[*Français*]

L'Office s'acquitte principalement de deux fonctions. D'abord, il s'agit d'examiner les activités relevant de la sécurité nationale et du renseignement afin de déterminer si elles sont légales, justes et nécessaires. Il ne faut pas confondre cela avec l'autorisation que mon collègue M. Noël accorde et dont il va vous entretenir un peu plus tard.

Ensuite, il s'agit d'enquêter sur les plaintes du public ayant trait à la sécurité nationale et au renseignement.

[*Traduction*]

Nous exerçons nos fonctions en toute indépendance, ce qui procure aux Canadiens l'assurance que les activités examinées sont conformes à la loi, notamment à la Charte. Le projet de loi C-22 introduit de nouveaux pouvoirs importants par l'entremise de la Loi sur le soutien en matière d'accès autorisé à de l'information, ou LSAAI. Compte tenu de l'étendue des nouveaux pouvoirs, l'OSSNR s'attendait à un rôle d'examen qui permette de constater rapidement et directement la façon dont ces pouvoirs sont exercés.

[*Français*]

Toutefois, dans sa forme actuelle, le projet de loi C-22 ne fournit à l'Office que le rapport annuel du ministre. Concrètement, cela pourrait signifier des délais de plus d'un an avant que l'Office soit en mesure de prendre connaissance de la façon dont lesdits pouvoirs sont exercés.

● (1845)

[*Traduction*]

Bien que l'OSSNR dispose de larges droits d'accès, il serait réellement utile que la loi impose que l'information soit communiquée à l'OSSNR en temps voulu et de façon proactive. Dans un contexte où les ressources sont limitées, une sensibilisation précoce permettrait d'établir une base de référence pertinente sur les activités en cours et permettrait à l'OSSNR de mieux planifier et de cibler plus efficacement ses activités d'examen.

[*Français*]

Nous accueillons favorablement la nécessité d'obtenir l'approbation du commissaire au renseignement pour ce qui concerne les arrêtés ministériels. Toutefois, l'absence de dispositions permettant à l'Office d'avoir accès à ces arrêtés ou l'absence de renseignements sur la façon dont ceux-ci sont mis en œuvre limitent notre capacité à en évaluer l'utilisation concrète.

Pour répondre à ces problèmes, nous recommandons deux modifications.

[*Traduction*]

Premièrement, nous proposons de modifier l'article 9 de sorte que l'OSSNR ait accès aux arrêtés ministériels classifiés délivrés aux fournisseurs de services, mais aussi aux renseignements fournis au commissaire au renseignement en appui à ces arrêtés.

Deuxièmement, nous proposons de modifier l'article 27 pour assurer que l'OSSNR soit tenu au courant lorsque des ordres de conformité sont émis, ce qui comprend les renseignements pertinents ayant trait à la non-conformité potentielle. Ces modifications permettraient de réaliser promptement et efficacement des examens mieux ciblés.

[*Français*]

De plus, ces modifications sont cohérentes avec d'autres lois canadiennes, suivant lesquelles l'Office reçoit de façon proactive des informations concernant les activités menées en vertu d'une autorisation ministérielle, et elles correspondent aux pratiques reconnues internationalement.

Il y a aussi des dispositions de cette nature en Australie. Vous pourriez poser des questions là-dessus.

[*Traduction*]

En conclusion, l'examen indépendant est l'un des piliers sur lesquels repose la confiance du public. Veiller à ce que l'OSSNR ait accès en temps opportun aux informations pertinentes favorisera la responsabilisation et concrétisera l'intention du Parlement au moment d'officialiser les pouvoirs dont il est ici question.

[*Français*]

Je vous remercie de votre attention.

Nous sommes prêts à répondre à vos questions.

[*Traduction*]

Le vice-président (Frank Caputo): Mme Deschamps siégeait à la Cour suprême du Canada lorsque j'étais étudiant en droit. Je ne peux tout simplement pas l'interrompre.

Des voix: Ha, ha!

[*Français*]

Le vice-président (Frank Caputo): Monsieur Noël, vous avez la parole pour cinq minutes.

L'hon. Simon Noël (commissaire au renseignement, Bureau du commissaire au renseignement): Monsieur le président, membres du Comité, je vous remercie de m'avoir invité à participer à vos travaux.

Je suis accompagné aujourd'hui de Justin Dubois, directeur général et avocat général de mon bureau.

Le projet de loi C-22 confère à mon bureau une nouvelle fonction importante. Je souhaite expliquer comment cette fonction s'inscrit dans le cadre de mes fonctions actuelles.

[*Traduction*]

Ma fonction quasi judiciaire en tant que commissaire au renseignement, ou CR, consiste à approuver ou non certaines activités de sécurité nationale et de renseignement proposées par le Centre de la sécurité des télécommunications, ou CST, et le Service canadien du renseignement de sécurité, ou SCRS, et autorisées respectivement par le ministre de la Défense nationale et le ministre de la Sécurité publique.

Mon approbation indépendante est nécessaire parce que les activités autorisées par les ministres peuvent être contraires à la loi ou porter atteinte aux attentes raisonnables en matière de vie privée des Canadiennes et des Canadiens. Je dispose de 30 jours pour rendre mes décisions, mais je m'adapte à des délais beaucoup plus courts lorsque la situation l'exige. Les activités ne peuvent être menées qu'avec mon approbation.

Lorsque j'approuve une autorisation ministérielle, j'évalue si les conclusions du ministre sont raisonnables au regard des facteurs que la loi l'oblige à prendre en compte, notamment l'incidence sur la vie privée et la cybersécurité. Pour la plupart de mes décisions, ma préoccupation principale est l'effet des activités proposées sur la vie privée des Canadiennes et des Canadiens. J'applique les principes juridiques de proportionnalité et de caractère raisonnable, et je veille au respect de la Charte, notamment de l'article 1.

● (1850)

[*Français*]

À cet égard, lorsque j'examine les facteurs que le ministre doit prendre en compte au moment de prendre un arrêté en vertu de ce projet de loi, je suis certain que ces arrêtés ressemblent grosso modo aux décisions ministérielles que je supervise actuellement, et ils soulèvent des questions juridiques que mon bureau connaît fort bien.

D'après mon expérience en tant que commissaire, je comprends que certaines ordonnances ministérielles ne peuvent être efficaces que si elles demeurent confidentielles. Bien que j'exerce mes fonctions dans un environnement classifié, mon rôle de surveillance m'impose d'être aussi transparent que possible envers les Canadiennes et les Canadiens. Je transmets mes décisions à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, présidé par M^{e} Deschamps, à des fins d'examen à postériori. Je publie des versions caviardées de mes décisions sur le site Web de mon bureau. Les décisions rendues en vertu du présent projet de loi seraient également publiées.

Mon rapport annuel, déposé au Parlement vendredi dernier, fournit également des informations sur l'incidence des activités que je supervise et sur les importantes questions de droit qui sont en jeu.

[*Traduction*]

Mon bureau aura-t-il besoin de ressources supplémentaires pour assumer cette nouvelle fonction? Je n'ai aucun contrôle sur le nombre d'ordonnances ministérielles que j'aurais à examiner ni sur la complexité ou le volume de chaque dossier. Il faut également tenir compte de l'effet potentiel des contrôles judiciaires. Ces considérations pourraient avoir une incidence sur les ressources dont mon bureau a besoin. Mon rôle est à temps partiel et j'adapte mon travail en conséquence. Je m'attends à ce que, si mon bureau nécessite des fonds supplémentaires, ceux-ci soient fournis en temps opportun. J'apprécierais certes un engagement ferme en ce sens de la part du ministre.

Un élément que je souhaite soumettre à votre réflexion concerne la possibilité pour le ministre de prolonger la période de validité d'un arrêté. À l'heure actuelle, aucune limite n'est imposée quant à la durée de validité d'une ordonnance ni à la durée d'une prolongation. Dans le cadre de mes attributions actuelles, des périodes de validité maximales sont précisées et les renouvellements requièrent une nouvelle approbation du CR. Je suggère d'adopter une approche similaire dans ce projet de loi.

[*Français*]

Je serai heureux de répondre à vos questions.

Le vice-président (Frank Caputo): Merci beaucoup, monsieur Noël.

[*Traduction*]

Nous sommes un peu en retard, alors je vais proposer, du moins pour ce tour-ci, de passer à cinq minutes par intervenant. J'espère que cela vous convient. Je ne voudrais pas que quiconque perde son tour.

Sur ce, nous allons commencer par M. Lloyd, pour cinq minutes.

Dane Lloyd: Merci.

Je remercie les témoins de leur présence ici.

Madame Deschamps, avez-vous été consultée pendant la rédaction de ce projet de loi?

L'hon. Marie Deschamps: Je crois comprendre que cette question a été posée au ministre.

Conformément à la loi, je rencontre le ministre une fois par année. Lorsque nous nous sommes rencontrés en décembre dernier pour notre réunion annuelle, le projet de loi C-22 n'a pas été abordé.

Dane Lloyd: Sur le plan philosophique, l'une des raisons pour lesquelles le Canada est un pays si remarquable, c'est précisément le sens des responsabilités dont nous faisons preuve — des couches redondantes de responsabilité. C'est pourquoi je suis vraiment choqué qu'il s'agisse de la deuxième version de ce projet de loi. Il y a eu le projet de loi C-2 et voici maintenant le projet de loi C-22. Des éléments de base en matière de responsabilité, dont des dispositions d'examen, ne sont pas là, comme vous l'avez dit. Je suis très frustré, compte tenu de la gravité des problèmes que ce projet de loi vise à régler. Il s'agit de choses comme l'exploitation sexuelle des enfants, et des mesures d'imputabilité de base comme un examen en sont absentes.

Pourriez-vous nous parler des raisons importantes pour laquelle l'Office de surveillance des activités en matière de sécurité nationale et de renseignement devrait participer au processus d'examen?

L'hon. Marie Deschamps: À l'OSSNR, nous recevons régulièrement de l'information sur les autorisations, et nous ne les ignorons pas. Nous les intégrons à nos connaissances sur les activités menées par les organismes. Grâce à ces connaissances, nous accumulons la somme d'information dont nous avons besoin pour planifier nos activités et mieux comprendre le fonctionnement des organismes.

Il est très important pour nous d'obtenir l'information le plus tôt possible, surtout dans le contexte de ce projet de loi. Nous en avons besoin dès que le commissaire au renseignement donne son approbation.

● (1855)

Dane Lloyd: Merci. J'espère sincèrement que nous pourrons discuter plus en profondeur d'amendements comme ceux que vous avez proposés. Je suis très frustré que cela ne figure pas déjà dans le projet de loi soumis par le ministre de la Sécurité publique.

Madame Curran, j'ai déjà posé cette question à un autre témoin. Meta divulgue-t-elle ses contrôles de protection de la vie privée à ses consommateurs?

Rachel Curran: Oui. Nous avons un centre de transparence où toutes nos politiques en matière de protection de la vie privée sont décrites. Nous intégrons essentiellement la protection de la vie privée dès la conception à tous nos produits, et nous expliquons très clairement à tous les utilisateurs quelles sont ces politiques.

Dane Lloyd: Si vous receviez l'ordonnance ministérielle secrète d'installer une fonctionnalité ou de créer une fonction permettant aux forces de l'ordre de contourner les contrôles de protection de la vie privée annoncés, comment pourriez-vous dire à vos utilisateurs que les choses que vous annoncez ne sont plus possibles?

Rachel Curran: Nous ne le pourrions pas, et c'est un problème majeur.

Je vais laisser ma collègue, Mme Greene, vous en parler plus en détail, car il s'agit d'une question importante.

Robyn Greene (directrice, Vie privée et politiques publiques, Meta Platforms Inc.): Merci beaucoup d'avoir posé cette question.

Dans sa forme actuelle, le projet de loi contient une disposition générale sur la confidentialité qui nous empêcherait essentiellement d'expliquer à nos utilisateurs que ces changements ont été apportés et, si on les découvrait, pourquoi ils l'ont été. Cette dernière partie est fondamentale parce qu'au bout du compte, nos services sont offerts partout dans le monde. Cela signifie qu'il y a constamment des chercheurs en sécurité, des experts techniques et des journalistes partout dans le monde qui décompilent nos produits et en font la rétro-ingénierie. Parfois, c'est parce qu'ils essaient de trouver des vulnérabilités et de nous aider à renforcer nos systèmes au moyen de programmes de chasse aux bogues. Parfois, c'est qu'ils essaient de voir s'ils peuvent obtenir des renseignements sur notre prochain produit ou nos prochains déploiements. C'est la même chose pour toutes les entreprises comme la nôtre.

Ce genre de changement finit toujours par être découvert. La question n'est pas « si ». Comme Mme Curran le disait, lorsqu'il s'agit d'exploiter une vulnérabilité, la découvrabilité est une question de « quand ». Les fournisseurs se retrouveraient alors en grave situation de conflit d'intérêts, car les utilisateurs perdraient complètement confiance dans la sécurité de nos produits et la protection de la vie privée que nous offrons.

Dane Lloyd: Je suis désolé de vous interrompre, mais mon temps est limité.

Apple a menacé de quitter le Royaume-Uni en raison de ses lois. Pensez-vous que de grandes entreprises pourraient également devoir quitter le Canada à cause de ce projet de loi, s'il n'est pas modifié?

Robyn Greene: Je ne peux pas vous dire ce que les autres entreprises vont faire, mais je pense qu'un certain nombre de dirigeants d'entreprises ont déclaré publiquement qu'ils n'étaient pas ouverts...

Le vice-président (Frank Caputo): Merci beaucoup. Je suis désolé, mais je dois vous interrompre.

Nous passons maintenant à M. Zuberi, pour cinq minutes, s'il vous plaît.

[*Français*]

Sameer Zuberi: Je remercie les témoins d'être ici.

[*Traduction*]

Je suis très heureux de vous voir devant nous aujourd'hui. J'ai beaucoup de respect pour le travail que vous avez accompli tout au long de votre carrière.

Je vais commencer par vous, monsieur Noël. Depuis longtemps, je vois les fruits de votre travail sur les certificats de sécurité et de nombreuses autres lois sur la sécurité nationale, et j'ai beaucoup de respect pour cela.

Vous avez dit plus tôt que l'une de vos principales fonctions concerne la protection de la vie privée et la perspective de la protection de la vie privée dans ce projet de loi. Diriez-vous qu'il serait le moindrement utile que le commissaire à la protection de la vie privée participe à cet exercice législatif?

L'hon. Simon Noël: Je ne sais pas exactement ce que contient la loi sur la protection des renseignements personnels, mais je pense qu'il suit déjà le travail que je fais — par l'entremise de son personnel. Je pense qu'il ferait la même chose dans mon cas. La distinction à faire entre le commissaire à la protection de la vie privée et moi est la suivante: je participe au processus décisionnel, tandis que le commissaire à la protection de la vie privée ne participe à aucune décision du gouvernement.

Sameer Zuberi: Je comprends.

À l'heure actuelle, les Canadiens s'attendent à une protection raisonnable de la vie privée. Ce projet de loi va changer la donne. Pouvez-vous nous expliquer en quoi cela changerait le paysage?

Les Canadiens peuvent-ils encore s'attendre à une protection raisonnable de la vie privée, compte tenu de la portée de ce projet de loi?

● (1900)

L'hon. Simon Noël: Il est difficile de prédire ce que l'avenir nous réserve. En cette nouvelle ère dans laquelle nous vivons, l'époque de l'annuaire téléphonique que les organisations policières pouvaient consulter est révolue depuis longtemps. Quelques groupes comme Meta contrôlent toute cette information. Le gouvernement doit maintenant trouver des moyens d'améliorer le système d'enquête partout au Canada.

[*Français*]

Il essaie d'établir un cadre, une architecture pour pouvoir le faire.

[*Traduction*]

Je vous dirais, monsieur, que les Canadiens, lorsqu'ils entendent parler des cas de pédophiles et de fraude bancaire, s'attendent à ce que le système s'adapte à la nouvelle réalité. Il faut prendre des mesures. C'est une proposition. Certaines personnes n'aiment pas la partie 2, mais quelqu'un, un moment donné, devra décider comment les banques de données qui sont essentielles aux organisations policières seront utilisées, et c'en est un exemple.

Sameer Zuberi: Je sais que vous avez parlé du devoir de franchise du SCRS et d'autres organismes. Je comprends que votre rôle actuel est différent de celui que vous occupiez avant, mais, madame Deschamps ou monsieur Noël, si vous avez des commentaires à faire au sujet des préoccupations qu'on pourrait avoir concernant le devoir de franchise ou de conformité des organisations policières et de ceux qui détiennent des pouvoirs... Craignez-vous que tout cela suscite des préoccupations?

L'hon. Simon Noël: Mon expérience, comme vous l'avez souligné, m'a appris à appeler les choses par leur nom: un manquement au devoir de franchise. Dans mon poste actuel, j'impose aux deux organismes le fardeau de me dire tout ce qu'ils vont me présenter, de m'en informer. S'ils ne me disent pas exactement ce que je devrais savoir ou ce que je ne sais pas, ils vont payer pour, parce que la décision ne penchera pas en leur faveur.

Sameer Zuberi: Je vais utiliser le reste de mon temps de parole pour implorer Meta de créer un environnement en ligne qui soit favorable à la famille, et honnêtement, pas seulement favorable à la famille, mais un environnement qui invite les gens à participer de façon positive. En tant qu'élus, nous recevons tellement de commentaires sur nos médias sociaux qui ne créent pas un environnement propice à la discussion positive.

Je tenais simplement à vous en faire part. Merci.

Le vice-président (Frank Caputo): Merci, monsieur Zuberi. Votre temps est écoulé.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour cinq minutes.

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Je suis bien contente de vous entendre, madame Deschamps et monsieur Noël. Je pense que vous êtes les seuls francophones à avoir pris la parole en quatre heures depuis le début de la réunion. Donc, ça fait du bien à mes oreilles. Je voulais vous le dire.

Madame Deschamps, on peut dire que l'Office de surveillance des activités en matière de sécurité nationale et de renseignement est une jeune organisation. Je pense qu'elle existe depuis environ six ans. J'ai l'impression d'être la députée qui encourage ses collègues à mieux connaître l'Office, parce qu'il est quand même assez méconnu. À force d'assister à vos breffages, je constate toute son importance en matière de protection et de surveillance.

Pour ce qui est du projet de loi C-22, le ministre ne semble pas comprendre ce que vous demandez et ce que je vais demander, à savoir que l'Office soit notifié. Il ne s'agit pas de demander que vous preniez part aux décisions. Nous savons que, suivant le projet de loi, c'est le travail du commissaire au renseignement.

Pourriez-vous nous expliquer pourquoi, en Australie ou dans d'autres pays, on a choisi de permettre à des agences équivalentes à la vôtre d'offrir une protection et une surveillance supérieures en leur permettant d'avoir accès aux informations en temps réel?

L'hon. Marie Deschamps: Je vous remercie de préciser ça. En écoutant certains des témoignages, j'ai eu l'impression qu'il y avait un peu de confusion quant aux rôles respectifs de l'Office et du Bureau du commissaire au renseignement.

Le commissaire au renseignement donne l'autorisation, au préalable, de procéder aux activités et, par la suite, les agences poursuivent leurs activités. Nous examinons, par exemple, la gouvernance de ces agences. Principalement, ce qu'on examine, c'est la légalité et le caractère raisonnable de leurs activités et si elles n'utilisent leur pouvoir que lorsque c'est nécessaire. Donc, nous examinons les activités après qu'elles ont été réalisées par...

● (1905)

Claude DeBellefeuille: Madame Deschamps, je suis désolée de vous interrompre, mais, comme vous le savez, je ne dispose que de cinq minutes.

Ça, on l'a bien compris quand vous avez fait votre allocution. Ce que je veux comprendre, et ce que je veux que vous expliquiez aux gens, c'est le fait que des pays ont fait un choix différent de celui que le gouvernement a fait dans le cadre du projet de loi C-22. Ces pays notifient, en temps réel, leur organisme de surveillance des décisions qui sont prises, par exemple, par un commissaire au renseignement.

Les Canadiens et les Québécois auraient avantage à savoir que l'Office est informé en temps réel, car cela les rassurerait. Si l'Office est informé un an après les faits, ça demande un gros effort en matière d'enquête. De plus, il n'est pas nécessairement doté d'une grande équipe qui lui permettrait de déterminer rapidement que les gestes posés n'étaient pas conformes aux règles.

Est-ce que j'ai bien compris?

L'hon. Marie Deschamps: C'est exactement cela.

Par exemple, en Australie, le délai est de quelques jours seulement. Ça évite aux organismes qui font la surveillance des activités de renseignement d'avoir à demander de l'information.

Quand on est obligé de demander de l'information, ce n'est efficace pour personne. Il faut le faire à la pièce, auprès de chacune des agences concernées. Ça prend du temps pour l'organisme qui demande l'information, et ça prend du temps pour les agences qui reçoivent la demande. Alors, tout ce qu'on recherche, c'est une plus grande efficacité. Si on reçoit l'information automatiquement, ça évite tout ce processus.

Claude DeBellefeuille: Le ministre, lors de son témoignage, a dit que si on proposait un tel amendement, il serait peut-être un peu en désaccord. Selon ce que j'ai compris, il a l'impression que ça retarderait le processus. Cependant, je crois que ce ne serait pas le cas, parce que le gros du travail est fait par le commissaire au renseignement, qui a une responsabilité importante.

Cependant, si vous êtes là, que vous êtes au courant et que vous suivez le jeu, ça va vous permettre d'être plus efficace et plus rapide pour détecter les activités non conformes.

Il me semble évident, madame Deschamps, que, actuellement, les citoyens et les entreprises sont inquiets. L'Office serait un garde-fou de plus. Pourquoi s'en priver?

L'hon. Marie Deschamps: L'Office serait là, probablement, mais les choses évoluent tellement vite, surtout en matière technologique.

Ainsi, on serait là à un moment où l'information serait peut-être périmée. Ce que nous voulons, c'est de l'efficacité. Nous voulons épargner à toutes les équipes d'avoir à aller chercher de l'information, et nous voulons pouvoir nous préparer de façon plus efficace pour ce qui est d'examiner les activités qui ont été accomplies.

Nous voulons mieux nous préparer et être en meilleure position pour les examiner.

Claude DeBellefeuille: L'idée est que le gouvernement s'inspire du Groupe des cinq, mais il n'a pas toujours adopté leurs meilleures pratiques. En effet, il m'apparaît que l'Australie a de meilleures pratiques en matière de surveillance.

N'est-ce pas?

L'hon. Marie Deschamps: C'est ce que nous pensons par rapport à cet aspect, celui de la notification.

Le vice-président (Frank Caputo): Merci, madame DeBellefeuille et madame Deschamps.

[*Traduction*]

Nous passons maintenant à Mme Kirkland, à qui j'aurais dû donner la parole plus tôt.

Je m'en excuse. Vous avez cinq minutes.

Rhonda Kirkland: Ça va. Merci beaucoup.

L'un de mes collègues d'en face a utilisé ses 30 dernières secondes pour implorer Meta de limiter la liberté d'expression. J'aimerais utiliser mes premières secondes pour implorer Meta de ne pas limiter la liberté d'expression. Je commencerai par cela.

Madame Curran, vous avez été pressée de vous dépêcher à la fin de votre témoignage. Je veux vous donner 30 secondes pour répéter votre conclusion afin que nous puissions vraiment bien la comprendre.

Rachel Curran: Merci, madame Kirkland.

Nous n'avons que trois demandes à formuler, trois recommandations sur ce projet de loi. Supprimez l'obligation contraignant les entreprises à intégrer des outils de surveillance ou d'autres logiciels du gouvernement ou de tiers à leurs systèmes. Cela inclut notre entreprise. Renforcez la définition de « vulnérabilité systémique » afin d'exclure explicitement toute exigence qui affaiblirait ou compromettrait le chiffrement, rendrait obligatoire d'examiner le profil du client ou introduirait une faiblesse en matière de sécurité. Codifiez le mécanisme permettant aux entreprises de contester les ordres problématiques. Je pense que nous avons bien entendu que les protections conférées après coup ne sont pas des protections du tout. Voilà nos recommandations pour la partie 2.

Soit dit en passant, nous pensons que la partie 1 répond aux critiques qui ont été formulées au sujet de la partie 14 du projet de loi précédent, le projet de loi C-2. C'est un bon cadre, sous réserve de quelques ajustements, pour fournir aux forces de l'ordre les renseignements dont elles ont besoin pour mener des enquêtes. C'est vraiment la partie 2 qui pose problème dans ce projet de loi. Nous recommandons des changements assez importants et fondamentaux à cette partie.

● (1910)

Rhonda Kirkland: Merci beaucoup.

Je veux aussi vous donner un moment pour répondre aux commentaires du commissaire au renseignement.

Je comprends que nous sommes entrés dans une nouvelle ère. Les choses ont changé en ce qui concerne ce qui est accessible en ligne et ce genre de choses. La seule chose que vous voudrez peut-être commenter est la suivante: apparemment, vous contrôlez toute cette information, tout comme l'annuaire téléphonique auparavant.

Avez-vous quelque chose à dire à ce sujet?

Rachel Curran: Oui. Je vais demander à ma collègue, Mme Greene, de répondre à cette question.

Rhonda Kirkland: D'accord. Merci.

Robyn Greene: Bien sûr, nous ne contrôlons pas toute l'information.

Il y a une chose qu'il est extrêmement important de comprendre concernant les services que nous offrons, c'est que les gens utilisent nos services pour différentes choses. C'est pourquoi nous sommes fiers, en fait, d'être le plus grand fournisseur de services de communications chiffrées de bout en bout au monde. Au bout du compte, les gens dépendent énormément de mécanismes de communication sûrs et privés, que ce soit pour les amis et la famille, pour gérer leur entreprise ou pour diverses activités de la vie courante. La réalité, c'est que les gouvernements dépendent également du chiffrement de bout en bout pour mener leurs affaires, défendre leurs intérêts et représenter les électeurs.

L'idée que la technologie évolue si rapidement est l'une des choses les plus importantes auxquelles nous devons réfléchir. Le chiffrement est une technologie qui évolue très vite, mais pas de la façon qu'imaginent beaucoup de gens. L'une des nouvelles vagues de développement de la technologie de chiffrement repose sur la cryptographie postquantique. L'une des plus grandes menaces auxquelles nous allons être confrontés dans les prochaines années est la suivante: à mesure que nous voyons l'informatique quantique progresser, il doit y avoir des avancées similaires dans la cryptographie postquantique, car c'est le seul type de cryptographie qui sera résistant à la capacité de décrypter des renseignements précédemment chiffrés.

L'une des choses qui nous préoccupent dans ce projet de loi, c'est qu'il n'y a pas suffisamment de mesures de protection pour garantir que le chiffrement ne sera pas compromis ou qu'un mandat visant à déchiffrer le chiffrement ne sera pas imposé. Cela deviendra beaucoup plus dangereux si l'on veut mettre en place un accès sûr exceptionnel, ce qui est vraiment un paradoxe en soi. Ce n'est pas quelque chose de possible. Ce sera beaucoup plus difficile à l'avenir avec la cryptographie postquantique.

Rhonda Kirkland: Il y a tellement de choses à décortiquer ici, et nous n'avons pas le temps de le faire. J'aimerais pouvoir vous accueillir ici pour une autre heure.

Je vais poser une question simple à laquelle il vous suffira de répondre par oui ou par non.

Je pense d'ailleurs que vous l'avez déjà dit. Les plateformes mondiales qui exercent leurs activités au Canada s'exposeraient-elles à de nouveaux risques systémiques en se conformant au projet de loi C-22, en particulier du fait qu'elles seraient tenues de conserver ou de produire des métadonnées ou des renseignements sur les abonnés à grande échelle?

Robyn Greene: Selon le libellé actuel, c'est effectivement chose possible.

Rhonda Kirkland: Vous avez dit que certains points vulnérables seront exploités. Y a-t-il quoi que ce soit dans ce projet de loi qui protège les Canadiens à cet égard?

Robyn Greene: Il n'y a rien de suffisant. À l'heure actuelle, la disposition visant à s'assurer que les fournisseurs n'ont pas à se conformer à une obligation qui créerait une vulnérabilité systémique ne s'appuie pas sur un processus bien établi ou sur une portée et une définition suffisamment claires pour s'assurer que l'on n'introduit pas par le fait même cette vulnérabilité systémique que le projet de loi vise à prévenir.

Rhonda Kirkland: Merci beaucoup.

Frank Caputo: Merci beaucoup.

Merci, madame Kirkland.

Nous passons maintenant à M. Housefather pour une période de cinq minutes.

Anthony Housefather: Merci, monsieur le président.

Je vais essayer de modérer mon enthousiasme, même si ce n'est pas tous les jours que nous accueillons une juge de la Cour suprême.

Roman Baber: Étiez-vous à la faculté de droit?

Anthony Housefather: Oui, bien sûr.

[*Français*]

Maître Deschamps, je crois que vous avez déjà très bien exprimé ce que vous aviez à dire. Vous avez envoyé une lettre au président du Comité, M. Jean-Yves Duclos, le 16 avril 2026. Cette lettre contenait deux propositions d'amendement.

Si ces deux amendements étaient adoptés par le Comité et, éventuellement, intégrés dans le projet de loi, est-ce que ça vous suffirait, en ce qui concerne les éléments qui relèvent de votre organisation?

● (1915)

L'hon. Marie Deschamps: En un mot, oui.

Anthony Housefather: D'accord. C'est parfait.

Monsieur Noël, je vous remercie beaucoup d'être ici.

Vous avez parlé de la nécessité d'avoir des ressources supplémentaires. Ça, c'est sûr. Le projet de loi prévoit un mandat très important pour vous.

Y a-t-il des changements que nous devrions apporter? Si vous me dites que ce n'est pas votre rôle, je comprendrai.

Cependant, avez-vous des propositions pour améliorer le projet de loi, à part le fait d'augmenter vos ressources?

L'hon. Simon Noël: La seule chose que je recommande, c'est d'indiquer, au paragraphe 7(3) du projet de loi, à la partie 2, que la décision de prendre un arrêté à l'égard d'un fournisseur de services électroniques doit être prise en fonction d'une norme de raisonnabilité et de proportionnalité.

Pour m'expliquer très sommairement, l'alinéa 7(3)a) doit être mis en équilibre avec la question des « effets possibles de l'arrêté sur les personnes auxquelles le fournisseur de services électroniques fournit des services », à l'alinéa 7(3)d), et avec la question des « effets possibles de l'arrêté sur la protection de la vie privée et la cybersécurité », à l'alinéa 7(3)e).

Il faut qu'il y ait une mise en équilibre entre ces éléments. C'est pour ça que je parle de raisonnabilité et de proportionnalité.

Anthony Housefather: Pourriez-vous envoyer votre proposition d'amendement par écrit au Comité?

L'hon. Simon Noël: Oui.

Anthony Housefather: Merci beaucoup.

[*Traduction*]

Permettez-moi maintenant de m'adresser aux représentantes de Meta. Soit dit en passant, je vous remercie d'avoir fait tout ce chemin depuis Washington. Nous vous en sommes très reconnaissants.

Madame Curran, je sais que vous n'êtes pas venue d'aussi loin, mais je vous remercie également d'être ici.

Je ne pense pas qu'il soit possible de simplement laisser tomber la partie 2, mais je comprends votre requête. J'abonde tout à fait dans votre sens pour ce qui est de la clarté. Il faut, premièrement, une définition claire de ce qu'est une vulnérabilité systémique; et, deuxièmement, une précision quant au fait qu'une éventuelle ordonnance ne pourra pas vous obliger à faire quelque chose qui crée une vulnérabilité systémique.

Est-ce que cela apaiserait en grande partie vos préoccupations?

Rachel Curran: Si vous définissiez clairement la protection du chiffrement dans le projet de loi, cela aiderait beaucoup.

Anthony Housefather: Que personne ne va demander qu'un chiffrement de bout en bout soit supprimé...?

Rachel Curran: Exactement, et je sais que le gouvernement a dit que son intention n'était pas de supprimer ou d'affaiblir le chiffrement. Si c'est le cas, il faut l'indiquer clairement dans le projet de loi.

De plus, si vous incluez dans le projet de loi une disposition qui empêche le gouvernement de formuler une demande s'il a des motifs raisonnables de croire qu'elle créerait une vulnérabilité systémique... À l'heure actuelle, la responsabilité incombe entièrement aux entreprises. C'est à nous de contester une demande et de dire que cela va créer une vulnérabilité systémique, et le processus pour le faire n'est pas tout à fait clair. S'il incombait au gouvernement de ne pas présenter des demandes qui, selon lui, créeraient une vulnérabilité systémique, cela contribuerait également beaucoup à apaiser ces préoccupations.

Anthony Housefather: Merci.

Je voulais également souligner que, bien sûr, on a beaucoup parlé des modalités d'utilisation de Meta. Après avoir lu ces modalités extrêmement longues, je dirais qu'il serait très facile d'ajouter une mise en garde pour dire que l'une des nombreuses exceptions à la protection de la vie privée que vous garantissez à l'utilisateur serait que la loi canadienne devrait, dans l'éventualité où telle et telle chose se produisent...

Permettez-moi de revenir en arrière pour profiter du fait que nous avons avec nous une experte des États-Unis. Pouvez-vous nous parler des principales différences entre les deux lois américaines et celle-ci?

Robyn Greene: La loi américaine, la Communications Assistance for Law Enforcement Act, est le fondement législatif en vertu duquel les fournisseurs de services de télécommunications et de services Internet sont tenus de veiller à ce que leurs services puissent être interceptés en réponse à des mandats d'écoute électronique.

Il y a des exceptions très clairement énoncées pour les services par contournement, comme ceux offerts par Meta et d'autres applications. Nous ne sommes pas soumis aux mêmes exigences. De plus, il y a dans cette loi des protections explicites pour le chiffrement. Une autre loi, la All Writs Act, n'offre pas non plus une voie claire et n'a jamais été désignée par les tribunaux comme étant un mécanisme qui permet de rendre obligatoire une option de contournement pour le chiffrement.

Le dernier point que j'aimerais soulever, c'est que ce sont les dispositions mêmes de la Communications Assistance for Law Enforcement Act qui ont mené aux vulnérabilités ayant rendu possibles les actes de piratage de Salt Typhoon et de Volt Typhoon.

Le vice-président (Frank Caputo): Merci beaucoup, monsieur Housefather.

[*Français*]

Madame DeBellefeuille, vous avez la parole pour deux minutes et demie.

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur le commissaire, dans un autre contexte législatif, vous avez développé une pratique de travail de proximité ou de collaboration avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. C'est déjà votre pratique.

N'est-ce pas?

● (1920)

L'hon. Simon Noël: Oui.

Claude DeBellefeuille: Vos deux bureaux travaillent ensemble.

L'hon. Simon Noël: Nous travaillons de manière complémentaire.

Claude DeBellefeuille: Si le gouvernement acceptait les amendements proposés, ça ne serait donc pas une surcharge pour vous. Ce serait la continuité d'une pratique que vous utilisez dans le cadre d'autres travaux.

Est-ce exact?

L'hon. Simon Noël: Il n'y aura pas de travail supplémentaire. Quand nous rendons nos décisions, madame DeBellefeuille, elles sont automatiquement transférées au bureau de Mme Deschamps.

Claude DeBellefeuille: D'accord. Ce travail est donc déjà fait.

L'hon. Simon Noël: Je ne veux pas parler pour Mme Deschamps, mais il s'agit juste de la décision. Il y a une tout autre documentation qui doit suivre, ce qui retarde un peu le travail. Nous n'avons pas de maîtrise là-dessus.

Claude DeBellefeuille: Je comprends.

J'ai vu les faits saillants de votre dernier rapport, monsieur Noël. Vous avez rendu 14 décisions au cours de la dernière année. C'est une année record. J'ai demandé aux fonctionnaires s'ils avaient évalué avec vous votre nouveau rôle sur le plan de la charge de travail et de l'intensité. En réponse à ma question, ils m'ont dit que vous vous êtes parlé et que ça devrait aller. Toutefois, vous avez dit d'entrée de jeu que c'est un peu de l'inconnu. Vous allez devoir vous ajuster un peu.

Votre expérience vous permet-elle d'avoir une idée de ce qui vous attend en matière de pression et d'intensité pour votre bureau?

L'hon. Simon Noël: Il est difficile de prévoir au juste comment...

Claude DeBellefeuille: Excusez-moi, mais je ne vous entends pas.

[*Traduction*]

Le vice-président (Frank Caputo): Mme DeBellefeuille a toujours la parole. Je vais arrêter le chronomètre.

Vous pouvez poursuivre, madame DeBellefeuille.

Merci.

[*Français*]

L'hon. Simon Noël: Je travaille à temps partiel.

Claude DeBellefeuille: Vous travaillez à temps partiel. Qu'est-ce que ça veut dire?

L'hon. Simon Noël: Je vais vous l'expliquer. C'est justement le point que je veux soulever.

Si je compare ma tâche à celle d'un juge, qui l'occupe à 100 %, actuellement mon travail m'occupe à 40 ou 42 %. Il y a encore du jeu. Il y a encore de la place. Je ne vois pas de problème, sauf que nous aimerions bien avoir un engagement lorsque nous verrons la façon dont le dossier se présentera.

Claude DeBellefeuille: Vous voulez que ce ne soit pas difficile à revendiquer.

N'est-ce pas?

L'hon. Simon Noël: C'est en plein ça. Nous ne voulons pas être obligés d'aller quêter.

Claude DeBellefeuille: Vous ne voulez pas être obligé de demander à M. Sabia de vous en donner un peu plus.

Est-ce bien ça?

L'hon. Simon Noël: Exactement. Nous ne voulons pas lui dire « s'il vous plaît, donnez-nous ça ». J'ai de l'indépendance et j'entends la préserver. Je n'irai pas quêter. Peut-être qu'il y aura d'autres moyens de pression à ce moment, comme retarder une décision qu'ils voudront obtenir bien vite.

Claude DeBellefeuille: Vous avez le gros bout du bâton.

Le vice-président (Frank Caputo): Merci de vos commentaires, monsieur Noël.

[*Traduction*]

Nous passons maintenant à M. Baber pour une période de cinq minutes

Roman Baber: Merci beaucoup, monsieur le président.

Bienvenue, monsieur le juge Noël.

Madame Deschamps, comme mes collègues, j'ai commencé mes études de droit la même année où vous avez été nommée juge à la Cour suprême. C'est vraiment un honneur de vous recevoir à notre comité.

Monsieur le juge Noël, je crois comprendre que le travail de commissaire au renseignement consiste essentiellement à approuver ou non certaines activités de renseignement et de sécurité. Est-ce exact?

L'hon. Simon Noël: Oui.

Roman Baber: J'ai également entendu certaines des observations que vous avez faites plus tôt à mes collègues. Avez-vous eu l'occasion d'examiner le projet de loi?

L'hon. Simon Noël: J'y ai jeté un coup d'œil. J'ai pris plus précisément connaissance de ce qui touchait mon rôle et de ce à quoi on s'attendait de moi.

Roman Baber: Comprenez-vous que l'on s'attendra à ce que vous approuviez les ordonnances du ministre de la Sécurité publique pour l'installation de systèmes de surveillance dans les entreprises privées? Comprenez-vous cela?

L'hon. Simon Noël: Je le comprends très bien. Ce n'est pas quelque chose de nouveau pour moi. Je suis au courant de beaucoup de choses...

Roman Baber: Je vois.

L'hon. Simon Noël: ... que je ne peux pas décrire en détail.

Roman Baber: Ce qui est important pour moi à ce stade-ci, c'est de savoir qui pourrait être visé.

J'ai demandé au greffier de vous remettre une copie du projet de loi.

L'hon. Simon Noël: Oui, je l'ai en main.

Roman Baber: Je vous demanderais d'aller directement à la page 36.

L'hon. Simon Noël: Oui.

Roman Baber: Je suis à la page 36, en bas à droite. On y donne la définition de « fournisseur de services électroniques » en indiquant qu'il s'agit d'une personne qui, seule ou au titre de son appartenance à un groupe, fournit des services électroniques au Canada ou exerce une partie de ses activités au Canada.

Il s'agit dès lors de savoir ce qu'est un service électronique, et la réponse est à la page suivante où il est écrit que « service électronique » s'entend de tout service — ou fonctionnalité d'un service — qui entraîne la création, l'enregistrement, le stockage, le traitement, la transmission, la réception, la diffusion ou la mise à disposition d'information sous forme électronique ou par d'autres moyens technologiques.

Cela me fait penser à un cabinet d'avocats qui a un serveur qui gère les courriels de ses clients. C'est un peu aussi comme une banque ou un cabinet de médecin.

● (1925)

L'hon. Simon Noël: Le secret professionnel...

Roman Baber: Cela va au-delà du secret professionnel. Il pourrait s'agir de votre boulangerie locale.

L'hon. Simon Noël: Je vois.

Roman Baber: Ma question est la suivante: croyez-vous que le commissaire au renseignement, dans le cadre de ses fonctions, devrait pouvoir rendre des ordonnances obligatoires pour l'installation, à la demande du gouvernement, de dispositifs électroniques permettant d'espionner les clients de n'importe quelle entreprise canadienne, et ce, sans qu'il y ait ordonnance du tribunal?

L'hon. Simon Noël: Il y a certains éléments que le ministre doit me fournir, et ils sont énoncés au paragraphe 7(3) proposé. Si j'ai un problème comme celui que vous soulevez avec cet exemple de la boulangerie, je serai amené à me poser d'importantes questions. Je veux simplement faire valoir que, sans connaître toutes les circonstances, il m'est impossible de savoir ce que je pourrais faire au bout du compte.

J'aimerais que vous sachiez qu'au cours de la première année de mon mandat à titre de commissaire, j'ai été exposé à des situations auxquelles je n'aurais jamais pensé être confronté et...

Roman Baber: Je comprends.

Si vous me le permettez, il ne me reste qu'environ une minute.

L'hon. Simon Noël: Je ne veux pas utiliser tout votre temps. Allez-y.

Roman Baber: Pour être juste avec tout le monde, mes amis libéraux ne souscrivent pas à notre interprétation de la loi. Ils croient que cela ne s'applique qu'aux fournisseurs de services Internet. Ce n'est pas ainsi que j'interprète la loi, mais je pense qu'ils ont droit à leur opinion.

Je suis curieux. Je ne veux pas que vous nous disiez combien de fois au fil des ans on vous a demandé d'approuver une ordonnance, mais sans violer la confidentialité, êtes-vous en mesure de m'indiquer quel est le taux de réussite du gouvernement lorsqu'il vous soumet une requête en ce sens?

L'hon. Simon Noël: Oui, je pourrais vous dire que je...

Roman Baber: Est-ce moitié-moitié... soixante-quarante?

L'hon. Simon Noël: Je vais vous en donner un aperçu. Mme De-Bellefeuille a parlé des 14 décisions que j'ai rendues l'an dernier. Je pense qu'il y en aura environ neuf cette année. J'ai dû signer près de 50 décisions depuis mon arrivée en poste et, de ce nombre, je dirais qu'environ 15 % des activités proposées ont été refusées.

Roman Baber: Vous dites bien 15 %?

L'hon. Simon Noël: Oui,15 %.

Roman Baber: Pour les 85 % restants, vous avez acquiescé à la demande du gouvernement.

L'hon. Simon Noël: Oui, mais on devrait parler du Centre de la sécurité des télécommunications et du ministère de la Sécurité publique, plutôt que du gouvernement lui-même.

Roman Baber: Je ne m'attendais pas à cela, mais je vous remercie de votre franchise.

Passons à Meta...

Le vice-président (Frank Caputo): Merci beaucoup, monsieur Baber. Malheureusement, nous avons dépassé le temps imparti.

[*Français*]

Le dernier député à prendre la parole ce soir est M. Ramsay.

Monsieur Ramsay, vous avez la parole pour cinq minutes.

[*Traduction*]

Jacques Ramsay: J'ai une question pour les représentantes de Meta.

Je crois comprendre que vous avez dit que le projet de loi, dans sa mouture actuelle, ne vous permettrait pas de protéger la vie privée des Canadiens. Diriez-vous en fait que si cette loi entre en vigueur, les Canadiens devraient fermer leurs comptes Facebook et Instagram?

Robyn Greene: Je ne dirais pas que c'est ce que nous avons voulu laisser entendre. Je pense qu'il faut surtout se préoccuper du fait que la loi, si elle est adoptée, confèrera au gouvernement le pouvoir de nous signifier des ordonnances qui pourraient fondamentalement violer les garanties de sécurité offertes par notre entreprise ou par tout autre fournisseur de services visé.

Jacques Ramsay: À la lumière de ce que vous venez d'entendre, à savoir que le commissaire au renseignement validera l'ordonnance du ministre et que vous pourrez ensuite demander une révision judiciaire en portant l'affaire devant les tribunaux, avez-vous toujours la même crainte?

Robyn Greene: Dans notre analyse de ce projet de loi, nous espérons obtenir un certain niveau de certitude juridique, non seulement pour nous-mêmes et notre capacité de mener nos activités commerciales, mais aussi pour nos utilisateurs afin de...

Jacques Ramsay: Je vous entends, mais je ne suis pas d'accord. Je pense qu'il y a pas mal...

Une voix: Cela n'aurait pas d'importance si...

Jacques Ramsay: Je suis désolé...

Le vice-président (Frank Caputo): Un instant, monsieur Ramsay.

C'est très difficile pour les interprètes, et je vous le dis alors qu'il m'est moi-même arrivé une ou deux fois d'interrompre un témoin, m'a-t-on dit, mais il s'agissait toujours de ministres.

Reprenons, s'il vous plaît.

[*Français*]

Monsieur Ramsay, veuillez poursuivre.

[*Traduction*]

Je vous demanderais de bien vouloir poser votre question au témoin.

Jacques Ramsay: La crainte de Meta, comme nos invitées l'ont d'ailleurs dit, c'est qu'il y ait des logiciels espions, d'une manière ou d'une autre.

● (1930)

[*Français*]

Monsieur Noël, si le ministre prenait un arrêté pour qu'on installe des logiciels espions, pourriez-vous donner un avis contre ça?

Meta semble craindre que le ministre abuse de ses pouvoirs.

L'hon. Simon Noël: Je peux vous assurer que ce serait un élément très important et que je regarderais cela sérieusement.

[*Traduction*]

J'aimerais rassurer les représentantes de Meta. Dans un cas semblable, vous pourriez me soumettre vos arguments que j'examinerais certes très sérieusement pour éclairer ma décision définitive.

Je sais en quoi consiste le chiffrement et à quel point il est important. Si quelqu'un essaie de contourner le chiffrement et d'ouvrir des voies d'accès à d'autres fins, je peux encore m'en remettre à mon bon jugement. Je sais ce que je fais. Mon intention, en fin de compte, est de protéger la vie privée des Canadiens, où qu'ils se trouvent.

[*Français*]

Jacques Ramsay: Monsieur le président, je n'ai rien d'autre à ajouter. Je vais donner le reste de mon temps de parole à Mme Acan.

[*Traduction*]

Le vice-président (Frank Caputo): Il semble que nous ayons un autre avocat ici.

Des députés: Oh, oh!

Le vice-président (M. Frank Caputo): Il vous reste deux minutes et 15 secondes.

Sima Acan: Merci beaucoup, monsieur le président.

Madame Greene, Meta se conforme déjà à la CLOUD Act des États-Unis, qui donne, comme vous l'avez mentionné, le pouvoir aux autorités américaines d'obliger les entreprises technologiques basées aux États-Unis à produire des données qu'elles ont en leur possession, sous leur garde ou sous leur contrôle, qu'elles soient stockées aux États-Unis, au Canada ou ailleurs dans le monde. En vertu de la CLOUD Act, les autorités américaines peuvent obtenir l'accès aux données des Canadiens, au moyen d'ordonnances judiciaires signifiées à des entreprises comme Meta, et Meta accepte ces obligations dans le cadre de ses activités aux États-Unis.

De même, le projet de loi C-22 exige un accès légal fondé sur une autorisation législative canadienne...

Le vice-président (Frank Caputo): Pourriez-vous ralentir un peu, s'il vous plaît, madame Acan, au bénéfice des interprètes?

Sima Acan: Je suis désolée.

De même, le projet de loi C-22 exige un accès légal fondé sur une autorisation législative canadienne et une surveillance judiciaire, mais Meta a soulevé d'importantes préoccupations au sujet de la proposition du Canada. Pouvez-vous expliquer pourquoi Meta considère qu'il est acceptable que les autorités américaines l'obligent à donner accès à ses données à l'échelle mondiale en vertu de la CLOUD Act, mais qu'elle s'y oppose alors que le Canada cherche à assurer ses propres...

Roman Baber: J'invoque le Règlement.

Je pense qu'il est très important, si ma collègue d'en face veut présenter un fait sur lequel elle s'appuiera pour soumettre un argument au témoin...

Sima Acan: Ce n'est pas un argument. C'est un fait.

Le vice-président (Frank Caputo): D'accord, laissons-le...

Roman Baber: Désolé, mais laissez-moi terminer mon rappel au Règlement.

Il faut que ce soit vrai et exact. Dans un cas, il s'agit d'une autorisation judiciaire. Dans ce cas-ci, il n'y a pas d'autorisation judiciaire. Voilà la différence.

Le vice-président (Frank Caputo): C'est peut-être...

Sima Acan: Il y a également une autorisation ici.

Le vice-président (Frank Caputo): Tout allait si bien.

Nous approchons de la fin de la soirée. Je sais que différentes personnes peuvent être en désaccord sur différents points et sur leur interprétation des choses. Je comprends votre point de vue, monsieur Baber. Je sais que Mme Acan essaie toujours d'être totalement honnête, alors c'est peut-être simplement...

Anthony Housefather: J'invoque le Règlement, monsieur le président.

Je suis désolé. Ce n'était pas un rappel au Règlement. Vous le savez très bien. Le témoin est tout à fait capable de répondre comme bon lui semble.

Roman Baber: Est-ce un véritable rappel au Règlement?

Le vice-président (Frank Caputo): D'accord, nous avons maintenant dépassé... Nous sommes en plein débat.

Madame Acan, pourriez-vous répéter votre question, s'il vous plaît?

Sima Acan: Merci beaucoup.

J'ai parlé de la CLOUD Act parce qu'il y a deux lois ici, qui ont les mêmes objectifs, et dans notre loi, nous avons aussi des ordonnances.

Il me reste encore du temps, n'est-ce pas?

Le vice-président (Frank Caputo): Oui, il vous reste une minute.

Sima Acan: D'accord.

Pouvez-vous expliquer pourquoi Meta considère qu'il est acceptable que les autorités américaines l'obligent à donner accès à des données à l'échelle mondiale en vertu de la CLOUD Act, mais qu'elle s'y oppose lorsque le Canada cherche à faire en sorte que ses propres organismes d'application de la loi puissent accéder légalement à des renseignements, en vertu des lois canadiennes, pour enquêter sur l'exploitation des enfants, la traite des personnes, le crime organisé et le terrorisme? Pourquoi les Canadiens devraient-ils accepter une situation où les autorités américaines peuvent accéder légalement à nos données, par l'entremise de Meta, mais où les forces de l'ordre canadiennes font face à des obstacles supplémentaires?

Le vice-président (Frank Caputo): Encore une fois, madame Acan, vous devez ralentir.

Sima Acan: C'était ma question. Merci.

Le vice-président (Frank Caputo): Vous avez 20 secondes pour répondre.

Robyn Greene: Ma réponse très courte est que la CLOUD Act ne prévoit pas ce que vous décrivez, et la loi américaine ne contient aucune disposition qui permettrait au gouvernement américain, avec ou sans ordonnance du tribunal, d'obliger les fournisseurs à aménager une voie d'accès pour le détournement du chiffrement ou à installer un logiciel de surveillance gouvernementale dans leurs systèmes. C'est notre principal sujet de préoccupation en ce qui concerne la partie 2.

La CLOUD Act permettrait un accès accru aux données sur les communications en vertu de la partie 1, et nous appuyons l'adoption de la partie 1, avec quelques amendements. Nous aimerions certes que le Canada conclue un accord en vertu de la CLOUD Act.

● (1935)

Le vice-président (Frank Caputo): Nous attendons avec impatience ces amendements.

Je sais que ces quatre heures ont été très longues.

[*Français*]

Je remercie les interprètes, les analystes, le greffier et les députés.

[*Traduction*]

Merci beaucoup. Je vous souhaite une excellente soirée.