CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

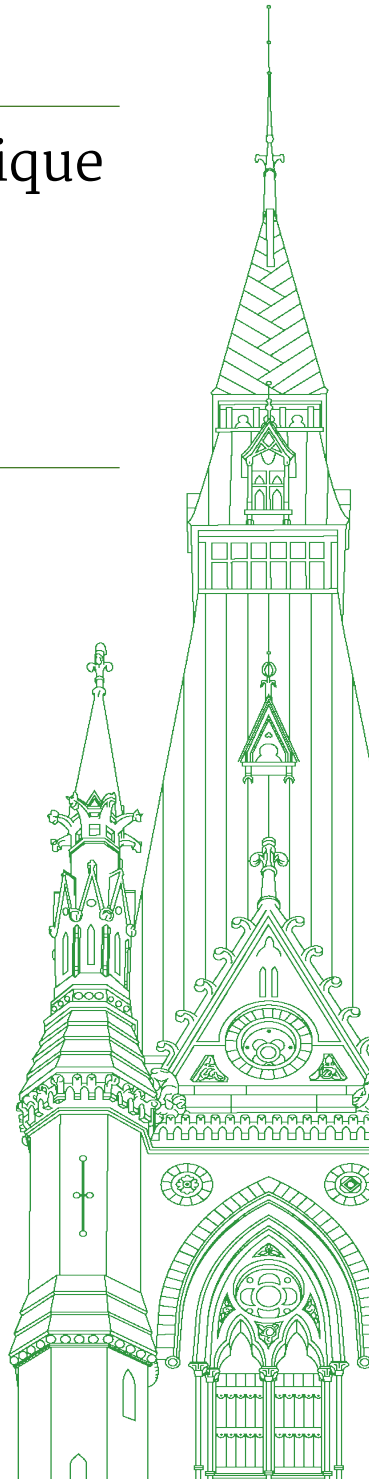
45e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 038

Le mardi 26 mai 2026



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le mardi 26 mai 2026

● (1545)

[*Français*]

Le président (L'hon. Jean-Yves Duclos (Québec-Centre, Lib.)): Bonjour à tous et à toutes. Je déclare la séance ouverte.

Je vous souhaite la bienvenue à la 38e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

Si vous le permettez, j'aimerais tout de suite proposer l'adoption des trois budgets qui ont été transmis par le greffier la semaine dernière. Il y en avait un pour l'étude du budget principal des dépenses, un deuxième pour le projet d'étude sur la gestion de la frontière Canada—États-Unis et un troisième pour l'étude du projet de loi C-22, étude que nous allons poursuivre aujourd'hui.

Comme vous le savez, les montants qui nous ont été transmis sont des estimations. Le Comité pourrait dépenser moins d'argent que ce qui est prévu. Toutes les sommes non dépensées seront retournées au Comité de liaison.

Si vous avez des questions, le greffier sera heureux d'y répondre.

Plaît-il au Comité d'adopter les trois budgets?

Des députés: D'accord.

Nous passons maintenant au sujet principal de notre rencontre d'aujourd'hui.

Conformément à l'ordre de renvoi de la Chambre des communes du 20 avril 2026, nous nous réunissons dans le cadre de l'étude du projet de loi C-22, Loi concernant l'accès légal.

Aujourd'hui, nous avons la chance d'accueillir de nombreux et distingués témoins, auxquels j'aimerais souhaiter la bienvenue.

Nous recevons les témoins du Barreau du Québec, à savoir Me Marcel-Olivier Nadeau, bâtonnier du Québec, qui est avec nous par vidéoconférence; Me Nicolas Le Grand Alary, avocat du Secrétariat de l'Ordre et affaires juridiques, qui est présent parmi nous; et Me Michel Marchand, membre du Groupe d'experts en droit criminel, qui est avec nous par vidéoconférence.

Nous recevons aussi M. Luc Lefebvre, président et cofondateur de Crypto Québec; ainsi que M. Philippe Dufresne et M. Marc Chénier, des Commissariats à l'information et à la protection de la vie privée du Canada.

Je souhaite à nouveau la bienvenue à chacun d'entre vous. Vous aurez la parole pour cinq minutes chacun pour faire votre présentation.

Maître Marcel-Olivier Nadeau, vous avez la parole.

Marcel-Olivier Nadeau (bâtonnier du Québec, Barreau du Québec): Merci, monsieur le président.

Mesdames et messieurs les membres du Comité, je vous remercie de nous recevoir aujourd'hui.

Je me présente. Je m'appelle Marcel-Olivier Nadeau, et je suis le bâtonnier du Québec. Je suis accompagné de Me Michel Marchand, membre du Groupe d'experts en droit criminel, et de Me Nicolas Le Grand Alary, avocat au Secrétariat de l'Ordre et affaires juridiques du Barreau.

Le Barreau du Québec vous remercie de nous avoir invités à participer aux consultations entourant le projet de loi C-22. Il est important de rappeler la mission du Barreau du Québec: assurer la protection du public, promouvoir une justice accessible et défendre la primauté du droit. C'est donc à ce titre que nous intervenons aujourd'hui.

D'entrée de jeu, permettez-moi de rappeler un principe fondamental. Le concept d'État de droit est au cœur de notre démocratie. Il exige que l'exercice des pouvoirs de l'État, notamment en matière d'enquête criminelle, soit encadré, prévisible et soumis à un contrôle judiciaire indépendant. Il commande également que les lois respectent les droits fondamentaux garantis par la Charte canadienne des droits et libertés, notamment le droit à la vie privée et à la protection contre les fouilles, les perquisitions et les saisies abusives. Cet équilibre n'est pas théorique. Il est essentiel pour maintenir la confiance du public envers nos institutions.

Le Barreau du Québec reconnaît l'objectif légitime du projet de loi, à savoir la modernisation des outils d'enquête dans un environnement numérique en constante évolution. Toutefois, nous sommes préoccupés par plusieurs dispositions qui risquent de porter atteinte aux droits fondamentaux, en particulier en matière de vie privée et de garanties constitutionnelles. Notre intervention vise donc à bonifier le projet de loi afin qu'il atteigne ses objectifs sans compromettre les principes au cœur du concept d'État de droit ni susciter des contestations judiciaires.

Nos recommandations s'articulent autour de quatre points principaux.

Premièrement, il y a une définition trop large du terme « renseignements relatifs à l'abonné ». Le projet de loi prévoit une définition qui est très large et qui est susceptible de révéler des aspects sensibles de la vie privée lorsqu'elle est combinée à d'autres données, comme le nom, le pseudonyme, l'adresse, le numéro de téléphone et l'adresse de courriel. La Cour suprême a d'ailleurs rappelé que l'analyse de l'attente raisonnable à la vie privée doit s'effectuer dans le contexte social et technologique actuel, selon lequel les données sont massivement collectées, croisées et conservées. Ainsi, même une information isolée peut acquérir un fort pouvoir révélateur lorsqu'elle est combinée à d'autres informations.

Par ailleurs, l'absence de définition précise de l'expression « personne fournissant des services au public » accroît les risques d'atteinte à la vie privée, car elle permet une interprétation large et des applications potentiellement abusives. En l'absence de balises législatives, cette formulation générique est susceptible de s'appliquer à un vaste nombre d'entités. Cela comprend non seulement les fournisseurs de services Internet, mais également des entreprises et des organisations détenant des renseignements personnels sensibles.

Cette formulation crée aussi une incertitude pour les entités visées, qui pourraient se voir contraintes de transmettre des informations sensibles sans savoir clairement si elles sont légalement tenues de le faire. Nous recommandons de clarifier et de restreindre ces définitions afin d'éviter qu'elles aient une portée excessive.

Deuxièmement, le projet de loi présente un seuil juridique insuffisant pour obtenir des ordonnances de communication. Selon le projet de loi, certaines ordonnances pourraient être autorisées sur la base de « motifs raisonnables de soupçonner », un seuil inférieur à celui généralement requis pour les atteintes à des droits fondamentaux.

Rappelons que la Cour suprême a établi que les renseignements relatifs à un abonné bénéficient d'une protection constitutionnelle élevée, ce qui justifie un contrôle judiciaire rigoureux. Nous croyons que, dans le projet de loi, le recours à une norme inférieure de simple soupçon, qui ne requiert pas la probabilité, mais seulement la possibilité raisonnable qu'une infraction a été ou sera commise, ne satisfait pas aux exigences constitutionnelles en matière de vie privée. Nous proposons donc que, comme pour les autres ordonnances du même ordre actuellement prévues par le Code criminel, le seuil de « motifs raisonnables de croire » soit considéré.

Troisièmement, il y a une absence de contrôles judiciaires applicables à certaines situations. En effet, dans certains cas, le projet de loi permet la communication volontaire de renseignements sans autorisation judiciaire, ce qui, à notre avis, constitue une rupture importante avec les garanties traditionnelles du droit criminel.

Rappelons que même les renseignements considérés comme des renseignements « de base », comme les coordonnées d'un abonné ou une adresse IP, peuvent, lorsqu'ils sont mis en relation avec d'autres éléments, permettre de dresser un profil détaillé de la personne concernée. Dans ce contexte, les tribunaux ont conclu que la communication de ces renseignements doit impérativement être accompagnée de garanties procédurales, notamment l'obligation d'obtenir une autorisation judiciaire préalable. Nous recommandons de supprimer ces mécanismes ou, à tout le moins, d'exiger un contrôle judiciaire préalable dans tous les cas.

● (1550)

Quatrièmement, la protection du secret professionnel et des données informatiques est mise à risque. Le projet de loi introduit des modifications utiles quant à l'examen des données informatiques. Nous considérons cependant qu'il devrait y avoir une condition prévoyant que l'extraction des données informatiques soit effectuée par une personne dont le seul rôle dans l'enquête relative à la commission de l'infraction visée est justement d'effectuer ladite extraction. Cela constituerait un moyen efficace d'éviter la contamination de l'enquête, et, par ailleurs, d'assurer la préservation du secret professionnel de l'avocat, qui constitue un principe de justice fondamentale au sens de l'article 7 de la Charte canadienne des droits et libertés.

Le président: Maître Nadeau, je vais devoir vous demander d'accélérer les choses.

Marcel-Olivier Nadeau: J'ai terminé, monsieur le président.

Pour conclure, je dirai que le Barreau du Québec invite les législateurs à réviser le projet de loi afin de maintenir un juste équilibre entre l'efficacité des enquêtes et la protection des droits fondamentaux.

Nous sommes prêts à répondre à vos questions.

Je suis désolé d'avoir légèrement dépassé mon temps de parole.

Le président: Je suis désolé de vous avoir interrompu. Si vous le souhaitez, vous aurez probablement l'occasion, plus tard, de préciser le dernier point que vous avez mentionné plus rapidement.

Monsieur Lefebvre, vous avez la parole pour cinq minutes.

Luc Lefebvre (président et cofondateur, Crypto Québec): Monsieur le président, membres du Comité, je me présente devant vous aujourd'hui au nom de Crypto Québec.

Lors de mon dernier passage devant ce comité, dans le cadre des consultations sur le projet de loi C-8, j'avais conclu mon intervention en disant que le modèle québécois permettait d'augmenter l'ensemble de la posture de sécurité, en harmonisant « sécurité » et « protection de la vie privée », et que le gouvernement devrait s'inspirer de cette approche, qui a déjà fait ses preuves.

[*Traduction*]

Or, nous nous retrouvons aujourd'hui devant un projet de loi que de nombreux professionnels de la sécurité de l'information du pays et d'ailleurs, ainsi que plusieurs organisations technologiques, considèrent comme assez dangereux. Il s'agit d'organisations dont les applications sont utilisées tous les jours par un très grand nombre de représentants canadiens élus ainsi que par les membres des forces de l'ordre. Je pense notamment à l'application Signal de la Signal Foundation, qui menace de quitter le pays advenant l'adoption du projet de loi, de manière à ne pas affaiblir le chiffrement de son application.

À notre avis, on devrait retirer le projet de loi et le repenser totalement. La prémisse de base du projet de loi est déficiente.

[*Français*]

Le projet de loi C-22 repose sur une prémisse qui n'a jamais été démontrée publiquement de manière rigoureuse, soit que le chiffrement constituerait aujourd'hui la menace centrale à la sécurité publique canadienne. Aucune preuve n'existe à ce sujet.

Nous avons entendu des anecdotes exprimées par certains corps policiers et certaines agences de renseignement, mais nous n'avons jamais vu de preuve empirique publique démontrant que le principal obstacle à la sécurité nationale canadienne est le chiffrement.

Au contraire, il a été démontré que, plus des données sont collectées, plus le risque de fuite quant à ces données augmente, sans réelle amélioration de la posture de sécurité.

[*Traduction*]

À ce sujet, aux États-Unis, il y a quelques années, le *Washington Post* a démontré que le FBI avait massivement surestimé le nombre d'enquêtes supposément bloquées par le chiffrement. Ces chiffres ont alors été utilisés publiquement pour justifier l'élargissement des pouvoirs de surveillance. Nous ne devrions pas répéter la même erreur au Canada.

On nous dit que le chiffrement est le problème, mais les rapports publics des agences de renseignement canadien elles-mêmes, ceux du CPSNR par exemple, nous informent principalement sur l'ingérence étrangère, l'insuffisance des ressources et l'expansion opaque de l'appareil de sécurité national. Le problème est donc assez clair. Il y a un manque de ressources humaines, techniques et financières ainsi qu'une augmentation excessive des pouvoirs de collecte de données sans réelles capacités de surveillance. Le projet de loi C-22 ne règle aucun de ces problèmes.

[*Français*]

Le chiffrement n'est pas le cœur de cette crise, il en est la solution.

Malgré tout, le projet de loi C-22 ne propose rien de moins que la création d'une infrastructure permanente de conformité à la surveillance numérique. Ce serait une infrastructure dans laquelle des fournisseurs de service pourraient être forcés de conserver plus de données, de maintenir des capacités techniques quant à l'accès, de répondre à des ordres secrets et de participer à des mécanismes d'extraction, et ce, même si le mot « *oversight* » apparaît exactement zéro fois dans le texte du projet de loi.

Le projet de loi ne parle pas non plus expressément de contre-pouvoirs démocratiques robustes. C'est extrêmement préoccupant. Une démocratie saine repose sur la vie privée, la liberté d'association, la confidentialité des communications et l'existence d'espaces où les citoyens peuvent échanger et critiquer le pouvoir sans craindre une surveillance structurelle permanente.

● (1555)

[*Traduction*]

Mon message pour les Albertains et les Québécois est le suivant: aucun gouvernement fédéral ne devrait jamais posséder des capacités structurelles élargies en matière de surveillance dans un contexte où les grands débats démocratiques et constitutionnels pourraient un jour opposer Ottawa et les provinces.

[*Français*]

L'histoire canadienne nous rappelle que les outils de sécurité nationale peuvent parfois déborder des menaces externes pour toucher des mouvements politiques internes. C'est précisément pourquoi les garde-fous démocratiques doivent être exceptionnels.

Il est également important de noter que si ce projet de loi passe dans son état actuel, tous les efforts effectués en matière de souveraineté numérique au Québec deviendront caducs.

[*Traduction*]

Protéger la démocratie au Canada exige des institutions solides qui concilient la sécurité et la protection des renseignements personnels avec un mécanisme de surveillance et des freins et des contrepoids robustes. Le projet de loi C-22, malheureusement, donne l'impression que la principale menace pour le Canada provient de plus en plus de l'intérieur plutôt que de l'extérieur. Nous savons tous que c'est une pente glissante pour une démocratie libérale.

Pour terminer, nous sommes d'avis que le Parlement canadien ne devrait pas adopter un projet de loi aussi fondamentalement transformateur en se fondant sur des hypothèses non fondées, des craintes ou des prémisses qui n'ont pas été démontrées publiquement. Il n'y a pas de porte dérobée utilisée uniquement par les bons. L'histoire de la cybersécurité nous montre précisément le contraire.

[*Français*]

Les probabilités de dérapages potentiels et les effets de ces derniers étant trop importants, nous demandons le retrait complet du projet de loi C-22.

Merci.

Le président: Merci, monsieur Lefebvre.

Monsieur Dufresne, vous avez la parole pour cinq minutes.

Philippe Dufresne (commissaire à la protection de la vie privée du Canada, Commissariats à l'information et à la protection de la vie privée du Canada): Merci, monsieur le président.

Mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invité à exprimer mon point de vue sur le projet de loi C-22.

La semaine dernière, j'ai soumis au Comité une communication écrite, que j'aborderai de façon plus détaillée aujourd'hui.

Le projet de loi C-22 réintroduit des dispositions sur l'accès légal qui avaient initialement été proposées dans le projet de loi C-2, mais avec plusieurs changements qui reflètent des commentaires que le gouvernement a reçus. Certains de ces changements concordent avec des recommandations écrites sur le projet de loi C-2 que j'ai présentées au ministre de la Sécurité publique en novembre dernier.

[*Traduction*]

Le projet de loi C-22 améliore celui qui l'a précédé, le projet de loi C-2, de plusieurs façons. Plus précisément, je me réjouis de la formulation plus précise de l'ordre de confirmer la fourniture de services. Je suis heureux de voir l'ajout des répercussions potentielles sur la protection de la vie privée et la cybersécurité parmi les facteurs à prendre en considération au moment d'élaborer des règlements et des ordonnances au titre de la Loi sur le soutien en matière d'accès autorisé à de l'information. Je suis également heureux de constater le nouveau rôle de surveillance confié par la Loi au commissaire au renseignement en ce qui concerne les arrêtés ministériels.

Cela dit, dans ma communication écrite présentée au Comité, j'ai noté certains aspects du projet de loi C-22 qui, à mon avis, devraient faire l'objet de nouvelles modifications visant à renforcer et à assurer la protection de la vie privée des Canadiens.

Plus particulièrement, je recommande de restreindre la définition de « renseignements relatifs à l'abonné » à une liste fermée d'identificateurs distincts, comme le nom, l'adresse, le numéro de téléphone et l'adresse IP de l'abonné. Cette approche permettrait d'éviter de recueillir des renseignements qui pourraient susciter des attentes accrues en matière de protection de la vie privée.

Je recommande également de limiter aux fournisseurs de services de télécommunications l'éventail de personnes ou d'entités qui pourraient être contraintes de communiquer des renseignements sur les abonnés ainsi que de veiller à ce que le juge de paix ou le juge qui rend l'ordonnance puisse préciser les renseignements relatifs à l'abonné qui doivent être communiqués.

[*Français*]

En outre, je recommande de définir l'expression « information accessible au public » de manière à exclure les renseignements à l'égard desquels une personne a une attente raisonnable en matière de protection de la vie privée, conformément à la définition figurant dans la Loi sur le Centre de la sécurité des télécommunications.

Le concept de renseignements dits « accessibles au public » continue d'évoluer, et un individu ne renonce pas automatiquement à toute attente raisonnable en matière de protection de la vie privée à l'égard de renseignements qui peuvent être accessibles en ligne. On peut penser, par exemple, à une situation où les renseignements d'un individu ont été communiqués à la suite d'une atteinte à la sécurité des données ou publiés à son insu ou sans son consentement.

[*Traduction*]

Une autre modification recommandée consisterait à ajouter une obligation générale selon laquelle les obligations imposées au titre de la LSAAI doivent être nécessaires et proportionnelles. Cet ajout contribuerait à faire en sorte que toute obligation de ce type, y compris celles liées à la conservation des métadonnées, soit adaptée pour réduire au minimum les répercussions sur la vie privée.

En ce qui concerne l'accès à l'information, je recommanderais de modifier la définition de « vulnérabilité systémique » afin de préciser qu'elle inclut toute action qui réduirait l'efficacité des méthodes systémiques d'authentification ou de chiffrement, comme dans la loi équivalente de l'Australie. De plus, je recommande de préciser que les règlements et les arrêtés ne doivent pas avoir pour effet d'exiger qu'un fournisseur de services électroniques introduise une vulnérabilité systémique ou d'empêcher un fournisseur de services électroniques de corriger une vulnérabilité systémique.

● (1600)

[*Français*]

Enfin, je recommande d'ajouter une exemption aux règles concernant la confidentialité énoncées dans la Loi sur le soutien en matière d'accès autorisé à de l'information, qui autoriserait expressément les fournisseurs de services électroniques à communiquer des renseignements aux organismes de réglementation appropriés, comme le Commissariat à la protection de la vie privée du Canada, afin de permettre à ces derniers d'exercer leurs attributions comme il se doit.

Je vous remercie de votre attention. Je répondrai à vos questions avec plaisir.

Le président: Je vous remercie tous les trois de vos présentations.

Monsieur Caputo, vous avez la parole pour six minutes.

Frank Caputo (Kamloops—Thompson—Nicola, PCC): Merci, monsieur le président.

Merci à nos témoins.

[*Traduction*]

Je vais commencer par le commissaire Dufresne. Encore une fois, merci d'être ici.

Pourriez-vous s'il vous plaît dire au Comité de quelle manière on vous a consultés pour l'élaboration du projet de loi?

Philippe Dufresne: C'est le ministre de la Sécurité publique qui nous a consultés à la suite de l'adoption du projet de loi C-2. Nous avons présenté quelques recommandations au ministre. Mon personnel s'est entretenu avec le personnel du cabinet du ministre. Nous avons eu l'occasion de présenter des commentaires. Certains d'entre eux ont été retenus; d'autres, non.

Frank Caputo: Ai-je raison de dire que vous, en tant que commissaire à la protection de la vie privée, n'avez pas été consulté sur ce qui devrait se retrouver dans un projet de loi qui touche la vie privée en ligne de tant de personnes?

Philippe Dufresne: Comme je l'ai dit, nous avons eu un échange. Nous avons été consultés après l'adoption du projet de loi C-2 sur ce à quoi devrait ressembler la prochaine version. Je ne dirais pas que nous n'avons pas été consultés dans ce cas-ci. Nous avons formulé un certain nombre de recommandations, dont certaines ont été adoptées, et j'ai souligné ces améliorations, mais un grand nombre d'entre elles n'ont pas été retenues: la nécessité et la proportionnalité, la sécurité, le resserrement de la définition…

Il subsiste des préoccupations en matière de vie privée, d'où le mémoire que j'ai adressé au Comité.

Frank Caputo: J'ignore si vous avez suivi le processus du Comité, monsieur le commissaire Dufresne. L'un des principaux problèmes que je vois ici, c'est la rapidité avec laquelle nous avançons.

Combien d'éminents témoins avons-nous ici? Nous avons six témoins très qualifiés qui représentent trois partis. Cela pourrait vraiment être divisé en deux groupes de témoins, à mon avis. Je ne pourrai même pas poser la moitié des questions.

Pourriez-vous vous exprimer à ce sujet? Avez-vous l'impression qu'on a pressé un peu trop les choses? Vous nous avez proposé cinq ou six amendements de fond. Nous n'allons même pas pouvoir vous questionner sur bon nombre d'entre eux parce que nous n'avons pas beaucoup de temps, sans même pouvoir aborder d'autres points valides. Selon votre observation, a-t-on précipité l'adoption de ce projet de loi?

Philippe Dufresne: Le Comité est le maître de ses délibérations, mais j'ai envoyé la semaine dernière un mémoire écrit, sachant que le temps était compté. Nous avons essayé d'en faire un document convivial et clair quant à ce que sont nos attentes. Nous présentons huit recommandations précises pour améliorer le projet de loi du point de vue de la vie privée.

Frank Caputo: J'en suis bien conscient. Je sais que vous ne pouvez pas vraiment vous prononcer.

Monsieur Lefebvre, vous avez observé ce processus. Ne vous semble-t-il pas précipité? C'est, du moins, ainsi que je le vois.

Luc Lefebvre: Tout à fait, il semble assez précipité, surtout sachant qu'il s'agit d'un projet de loi qui a une incidence sur tous les Canadiens.

On connaît la rengaine. Des pouvoirs extraordinaires s'accompagnent de responsabilités extraordinaires. J'ai l'impression qu'ils demandent des pouvoirs extraordinaires, mais nous ne savons pas pourquoi. Il semble que cela n'ait pas fait l'objet d'une profonde réflexion, car c'est quelque chose qui a des répercussions pour tout le monde. Nous comprenons que cette demande fait suite à des besoins et à des exigences des membres des forces de l'ordre et de nos agences du renseignement, mais les conséquences sont si importantes qu'elle doit faire l'objet de discussions ultérieures.

Frank Caputo: Je suis d'accord avec vous. Personne ne doute de notre volonté d'attraper les méchants, comme les terroristes, et — comme dans ma vie antérieure — ceux qui infligent des mauvais traitements aux enfants. Cela ne fait aucun doute.

Vous avez aussi frappé en plein dans le mille. Non seulement ce processus a-t-il été précipité, mais les communications du gouvernement ont été terribles, si vous voulez tout savoir. Le ministre ne voulait pas déclarer s'il serait ouvert à une modification du chiffrement, un élément que vous avez souligné. Je ne sais pas pourquoi nous utilisons de jolies formules comme « neutre sur le plan du chiffrement ». Nous ne savons rien à ce sujet.

Les amendements doivent être soumis demain, or nous entendrons les représentants jeudi. Nous n'avons eu qu'une seule heure avec les représentants. De votre point de vue, voyez-vous pourquoi il serait prudent d'étudier davantage ce projet de loi?

● (1605)

Luc Lefebvre: Comme je l'ai dit plus tôt, les répercussions sont importantes. Chaque pays qui l'a fait, parce qu'il y a d'autres pays du Groupe des cinq qui ont suivi cette voie… Si je pense à l'Australie et au Royaume-Uni, ils ont pris le temps de bien y réfléchir. Ils ont suivi une voie différente de celle que j'aurais aimée, mais ils ont pris plus de temps.

Cette question touche les entreprises. Elle touche tous les citoyens et tous les aspects de la vie quotidienne. Elle mérite qu'on s'y attarde davantage.

Frank Caputo: Je comprends.

Je suis désolé, mais je dois écourter mon échange avec vous, car il ne me reste qu'environ 45 secondes.

Monsieur Nadeau, vous avez notamment parlé de surveillance et du fait d'attraper des gens. En ce moment, le commissaire au renseignement doit approuver ou autoriser un arrêté ministériel. Quel est votre avis sur une modification qui exigerait une surveillance judiciaire? Autrement dit, plutôt que de passer par le commissaire au renseignement, ce serait la Cour fédérale du Canada… Au lieu d'avoir à recourir à un contrôle judiciaire comme étape supplémentaire, la demande serait directement soumise à la Cour fédérale du Canada pour ce qui est d'approuver un arrêté ministériel.

[*Français*]

Marcel-Olivier Nadeau: Je vous remercie de votre question, monsieur le député.

Je vais laisser notre expert, M^{e} Marchand, y répondre.

Michel Marchand (membre, Groupe d'experts en droit criminel, Barreau du Québec): Bonjour.

C'est une vaste question, à laquelle il est difficile de répondre. Il faudra voir quel est le contenu visé par l'arrêté ministériel. Il est difficile de répondre à la question sans connaître tous les paramètres.

Le président: Je vous remercie de cette réponse brève.

De toute manière, nous avons dépassé les six minutes prévues pour ce tour de parole.

Madame Acan, vous avez la parole pour six minutes.

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

[*Traduction*]

Monsieur Dufresne, la portée du projet de loi est de fournir des renseignements de base sur un particulier, et non sur le contenu de ses données, sur les pages qu'il consulte ou sur ce qui figure dans ses courriels. Le ministère a pris le temps d'étudier attentivement les préoccupations en matière de vie privée et les considérations liées à la Charte. Toutefois, nous avons entendu des inquiétudes selon lesquelles le libellé actuel de l'article proposé 487.011, « personne fournissant des services au public », pourrait englober des services autres que ceux des fournisseurs de services Internet.

En tant que commissaire à la protection de la vie privée, quelles modifications du libellé proposeriez-vous pour circonscrire la portée des services visés à l'article proposé 487.011 afin de dissiper ces préoccupations, tout en veillant à ce que les responsables des forces de l'ordre disposent des outils nécessaires pour accéder à l'information dont ils ont besoin?

Philippe Dufresne: En effet, il est important que le projet de loi concilie la nécessité pour les forces de police de disposer des outils dont ils ont besoin et de protéger la vie privée des Canadiens, et nous pouvons le faire. Ce n'est pas un jeu à somme nulle entre la vie privée et la sécurité. Nous répondons à ces préoccupations dans les trois premières recommandations de notre mémoire écrit.

En particulier, la première étape consisterait à restreindre la définition de « renseignements relatifs à l'abonné ». Il faudrait la modifier pour qu'elle ne couvre plus des notions plus larges comme les « renseignements permettant d'identifier » des personnes ou « les renseignements relatifs aux services fournis », et la ramener à des éléments précis tels que le nom, l'adresse, le numéro de téléphone et l'adresse courriel. Nous le précisons dans notre mémoire.

Ensuite, il faudrait restreindre l'éventail des entités qui peuvent obtenir ces ordonnances aux seuls fournisseurs de services de télécommunications. Cette limite existe déjà pour les demandes sans mandat visant la confirmation d'un service, mais pour ce qui est des renseignements relatifs à l'abonné, le texte actuel vise « une personne qui fournit des services ». À notre avis, c'est beaucoup trop large. Cela pourrait englober des cabinets médicaux ou juridiques et donner accès à une quantité importante de renseignements sensibles.

Enfin, il faudrait préciser davantage la portée de l'ordonnance du juge. À l'heure actuelle, le libellé indique « les renseignements relatifs à l'abonné » ou « tous les renseignements relatifs à l'abonné » liés à un élément donné, ce qui peut être très large. Nous proposons donc de resserrer cette formulation.

Je soulignerais un dernier élément concernant la perquisition sans mandat ou l'ordre de confirmer la fourniture de services. Il existe une exception pour les renseignements médicaux et privilégiés, mais cette exception est absente en ce qui concerne les renseignements relatifs à l'abonné.

Ce sont les recommandations que je formulerais.

Sima Acan: Merci beaucoup, monsieur Dufresne.

Pour poursuivre, nous avons également eu le privilège d'entendre l'Office de surveillance des activités en matière de sécurité nationale et de renseignement ainsi que le commissaire au renseignement, qui assure la reddition de comptes de notre régime de sécurité nationale. En revanche, en tant que commissaire à la vie privée, vous jouez un rôle important pour veiller à ce que les ministères et les organismes fédéraux respectent les pratiques de traitement des renseignements personnels.

Quel ajout recommanderiez-vous aux arrêtés ministériels pour faire passer ce projet de loi à la prochaine étape?

● (1610)

Philippe Dufresne: Je suis favorable à l'ajout du rôle d'examen du commissaire au renseignement. C'est une amélioration importante qui a été apportée, et j'y suis tout à fait favorable. Je pense qu'il est essentiel d'ajouter la nécessité et la proportionnalité à la portée des ordonnances qui pourraient être faites par le gouverneur en conseil et le ministre. C'est un concept du droit de la vie privée largement répandu dans le monde. En fait, les signataires de la déclaration sur l'accès gouvernemental aux renseignements du secteur privé de l'OCDE, en décembre 2022, ont réclamé unanimement et expressément la « nécessité » et la « proportionnalité ». C'est très important.

Je pense que le commissaire au renseignement Noël a également parlé du concept de caractère raisonnable et de proportionnalité. C'est une norme très importante. Le projet de loi comporte quelques dispositions exigeant de tenir compte des répercussions sur la vie privée. C'est une bonne chose, mais à mon avis, il faut aller plus loin pour garantir la nécessité et la proportionnalité.

Sima Acan: Merci, monsieur Dufresne.

Monsieur Nadeau, d'après ce que je comprends, vous aimeriez resserrer la définition de « renseignements relatifs à l'abonné ». Actuellement, à la partie 1 du projet de loi, un ordre de confirmer la fourniture de services pose une simple question par oui ou non pour déterminer si une personne utilise le service. De plus, la définition de « renseignements relatifs à l'abonné » à l'article proposé 487.011 porte sur les identifiants, autrement dit, les renseignements de base. Ce n'est pas le contenu des données, comme les pages que vous parcourez ou ce qui se trouve dans votre courriel.

Pourriez-vous expliquer ce que vous aimeriez que l'on ajoute à l'article proposé 487.011 pour restreindre la définition et la portée?

[*Français*]

Marcel-Olivier Nadeau: Je vous remercie de votre question.

Je pense que le commissaire, qui vient de s'exprimer, a donné d'excellents exemples. Je n'en aurais pas d'autres à ajouter, mais je permettrais à M^{e} Marchand ou à M^{e} Le Grand Alary, s'ils ont d'autres exemples à donner, de vous les fournir. Ceux qui viennent d'être donnés par le commissaire à la protection de la vie privée sont d'excellents exemples, et je les fais miens, tout comme les principes qu'il a énoncés.

[*Traduction*]

Sima Acan: Merci beaucoup.

[*Français*]

Nicolas Le Grand Alary (avocat, Secrétariat de l'Ordre et affaires juridiques, Barreau du Québec): Merci, monsieur le bâtonnier.

J'allais effectivement ajouter un point. À mon avis, le commissaire a bien expliqué en quoi consistaient les préoccupations. Il y a la notion de renseignements relatifs à l'abonné et, également, la notion de l'ordonnance de la cour. Ce sont tous ces éléments qui causent un problème, c'est l'ensemble de l'œuvre. Il faudrait resserrer les trois définitions. Je pense que monsieur le commissaire a bien expliqué la question.

[*Traduction*]

Sima Acan: Merci beaucoup, monsieur le président.

Mon temps est écoulé.

[*Français*]

Le président: Merci beaucoup, madame Acan.

Monsieur Lloyd, vous avez la parole pour six minutes.

Pardonnez-moi, c'est plutôt votre tour, madame DeBellefeuille. Je vous présente toutes mes excuses. C'est impossible de vous oublier, mais j'ai quand même réussi à le faire.

Vous avez la parole pour six minutes.

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

Je vous fais part de ma grande déception d'avoir si peu de temps de parole alors qu'un groupe de témoins si riche est présent.

Comme nous sommes pressés par le temps, nous allons essayer d'avoir des questions courtes et des réponses qui vont nous éclairer.

Personnellement, plus j'en apprends, plus je suis mêlée. En fonction de la personne à qui on parle, que ce soit un policier ou un représentant d'une association qui veut protéger la vie privée, on a des versions complètement divergentes et très polarisées. Notre but est de leur dire que c'est effectivement un projet de loi important et nécessaire, mais aussi de leur expliquer comment on va vivre cet équilibre.

Monsieur Dufresne, je suis toujours surprise de constater que vos recommandations n'ont pas été entendues avant la rédaction du projet de loi. Nous sommes toujours un peu en retard. Nous avons vécu cette situation par rappot au projet de loi C-8. Personne n'avait pris la peine de vous consulter. Maintenant, vous présentez des recommandations, et ce sont des partis d'opposition qui les soumettent à titre d'amendements au projet de loi. Je trouve ça curieux, surtout que nous n'avons pas beaucoup de temps pour en débattre. Nous aurions préféré que le gouvernement fasse bien son travail, qu'il vous écoute et inclue vos recommandations directement dans le projet de loi, parce qu'elles m'apparaissent raisonnables. Le projet de loi aurait été meilleur et nous aurions économisé du temps.

Monsieur Lefebvre, vous avez capté mon attention en disant qu'il a été prouvé aux États-Unis que, même avec un accès légal, il n'y a pas de baisse de la criminalité. Il n'y a aucune statistique. L'affaiblissement du chiffrement n'équivaut pas nécessairement à une diminution de la criminalité. Quand on écoute les policiers, c'est ce qu'ils nous disent, soit qu'ils seront plus performants, qu'ils arrêteront plus de criminels et qu'ils pourront contrer le crime organisé.

Vous semblez nous dire que l'équation n'est pas aussi évidente.

Pouvez-vous nous donner plus de détails là-dessus?

● (1615)

Luc Lefebvre: En fait, la tendance à vouloir encadrer ce qu'on appelle l'accès légal dans les différents pays du Groupe des cinq existe depuis 10 ou 15 ans. L'Australie et le Royaume-Uni, notamment, ont des lois qui sont particulièrement rigoureuses en matière de collecte de données dans le but avoué de combattre la pédocriminalité, les criminels, ce genre de choses.

Cependant, à ce jour, il n'y a aucune donnée démontrant que, plus on a des accès élevés et plus on influe sur le chiffrement des applications, des messageries et des différents outils utilisés, plus il y a une diminution associée à cette augmentation de pouvoir. La seule chose qu'on fait, au bout du compte, c'est accumuler plus de données sans diminuer la criminalité.

En fait, ce qu'on remarque, c'est que, plus les pouvoirs sont élevés, plus les criminels ont tendance à devenir invisibles. C'est ce qu'on appelle *going dark*. Ils utilisent d'autres méthodes et d'autres outils, et on finit, de toute manière, par perdre leur trace. Toutefois, on continue d'accumuler de plus en plus de données sur M. et Mme Tout-le-Monde, c'est-à-dire des gens qui ne sont pas liés à ces activités.

Claude DeBellefeuille: Prenons l'exemple du Royaume-Uni, dont on veut s'inspirer, ainsi que celui de la Nouvelle-Zélande ou de l'Australie. Le Royaume-Uni a même installé des caméras où les citoyens sont filmés pendant leur quotidien. On a poussé la surveillance à l'extrême.

A-t-on obtenu des résultats concernant la diminution du taux de criminalité?

Luc Lefebvre: On n'a pas établi de corrélation. Le Royaume-Uni est réputé pour avoir des caméras en circuit fermé partout, ce qu'on appelle des CCTV. De plus, le Royaume-Uni a adopté des lois extrêmement rigoureuses en matière de collecte de données et de liberté d'expression. Aucune corrélation n'a été démontrée entre cela et une diminution importante de la criminalité. Cependant, c'était l'excuse officielle qui était utilisée.

Claude DeBellefeuille: J'ai assisté à une réception de l'Association canadienne des chefs de police. J'ai vu une salle de gens très enthousiastes. Ils disaient que ça faisait 30 ans qu'ils attendaient une telle loi.

Pourquoi pensez-vous que le gouvernement est si pressé de faire adopter cette loi? Y a-t-il des pays qui nous incitent à aller dans ce sens?

Luc Lefebvre: J'aimerais dire deux choses.

Premièrement, c'est normal que les services de police soient heureux que ça arrive. Je viens d'une famille de policiers qui combattaient notamment la pédocriminalité. Je le comprends totalement, cet enthousiasme, et c'est nécessaire. Ça ne m'étonne pas de voir que les forces de police s'en réjouissent. C'est tout à fait louable.

Deuxièmement, nous avons surtout l'impression, en fait, que la pression vient d'autres membres, notamment du Groupe des cinq, qui cherche à obtenir de plus en plus de visibilité partout dans le réseau, ainsi que d'alliés. Le Canada est un peu à la traîne, justement, sur la capacité de donner accès à ces données. Il y a clairement une certaine pression politique qui se fait à cet égard.

C'est probablement la solution la plus simple pour le gouvernement. On dit qu'on va donner accès aux données des Canadiens aux forces policières en diminuant le chiffrement. Elles seront contentes. C'est la solution facile au lieu d'augmenter, par exemple, les ressources financières, techniques et humaines pour combattre le crime. Parallèlement, nos alliés seront contents. C'est l'impression que nous avons.

Claude DeBellefeuille: Monsieur Dufresne, comme vous le savez, nous avons jusqu'à demain soir, 17 heures, pour déposer nos amendements.

Vos recommandations sont-elles déjà libellées sous forme d'amendements pour que nous puissions les utiliser et les déposer?

Philippe Dufresne: Elles ne sont pas rédigées comme le bureau du légiste peut le faire, mais elles sont rédigées dans notre mémoire de façon à ce que ce soit facile, à mon avis, de les transformer en amendements.

Nous faisons des renvois à des exemples qui existent déjà, par exemple la loi de l'Australie, où on précise que ça ne doit pas avoir l'effet, par exemple, de diminuer la capacité de chiffrement. On vient apporter une modification. Un des articles qui nous préoccupe dans le projet de loi, c'est celui où on dit qu'un fournisseur n'a pas besoin de se conformer à une ordonnance.

Nous pensons qu'il serait important de dire qu'on ne devrait pas faire l'ordonnance du tout. Ça met le fournisseur dans une situation difficile. On lui ordonne de faire quelque chose, mais la loi lui permet de désobéir. Je pense qu'on devrait le faire comme il faut dès le début.

Nous avons abordé le principe « nécessité et proportionnalité ». Nous avons parlé de la Grande-Bretagne, qui applique ce principe. L'Australie le fait aussi. C'est un principe de base, alors ce n'est pas compliqué. On peut l'ajouter dans les motifs à considérer par le ministre ou par le gouverneur en conseil.

Je pense que les huit recommandations que nous proposons sont ciblées. Elles sont concises, et elles visent essentiellement à atteindre cet équilibre fondamental.

● (1620)

Claude DeBellefeuille: Merci beaucoup, messieurs.

Le président: Merci beaucoup, madame DeBellefeuille.

[*Traduction*]

Dane Lloyd (Parkland, PCC): J'invoque le Règlement.

Le président: Allez-y, monsieur Lloyd.

Dane Lloyd: Merci, monsieur le président. Je voulais attendre que ma collègue, Mme DeBellefeuille, ait terminé.

J'ai entendu le commissaire à la vie privée nous parler d'un mémoire qu'il a présenté au Comité. Je pense que celui-ci a été envoyé au président le 21 mai. Nous ne l'avions pas reçu avant aujourd'hui.

Je ne cherche pas à attribuer de mauvaises intentions à qui que ce soit, mais ma capacité, en tant que parlementaire, d'analyser ce projet de loi et d'être préparé à la réunion d'aujourd'hui a été vraiment compromise. En ne recevant pas les documents envoyés par les témoins, je n'ai pas la capacité de les examiner correctement.

Par ailleurs, nous n'avons toujours pas reçu la transcription de notre réunion d'il y a deux semaines. Je viens de le mentionner à notre greffier, qui nous assure que cela s'en vient. Vous savez, nous avons eu une pause de deux semaines. Si nous ne sommes pas en mesure d'obtenir des renseignements essentiels pour nous aider dans ce processus, compte tenu de la nature précipitée du processus législatif que nous sommes en train de mener… J'ai de sérieuses réserves quant à la vitesse avec laquelle ce processus avance, car nous ne recevons pas des informations et des preuves adéquates pour mener à bien ce projet de loi.

Le président: Merci. Ce n'est pas exactement un rappel au Règlement. Vous soulevez plutôt une question de privilège, mais je pense que nous en comprenons la valeur.

Le greffier vient de m'informer il y a quelques minutes qu'il n'a pas été en mesure de l'envoyer plus tôt, pour des raisons humaines. Il tient à exprimer son malaise devant cette situation. Il l'a maintenant reçu, et je vous encourage donc tous à consulter vos courriels. Le document complet vient d'être communiqué.

En ce qui concerne la transcription, il faudrait peut-être que je sache un peu mieux ce que le greffier doit fournir, par souci de précision.

Monsieur le greffier, allez-y.

Le greffier du Comité (Paul Cardegna): Merci, monsieur le président.

Pour ce qui est de la transcription, nous avons été informés que le service des publications de la Chambre des communes a établi des normes de service. Je peux les examiner et revenir avec l'information au Comité, car je ne les ai pas avec moi en ce moment. Cependant, il m'a écrit vendredi pour me faire savoir qu'il y avait quelques retards, nonobstant la durée de la réunion du 7 mai, qui a duré quatre heures plutôt que deux, ainsi que l'important volume de dossiers qui passent également par son bureau. On m'a indiqué qu'il travaille aussi fort que possible pour produire cette transcription.

Je peux vous envoyer les bleus dès maintenant, monsieur Lloyd, et je le ferai. Ils sont habituellement accessibles à l'intérieur du pare-feu. Si un député n'y a pas accès, nous pouvons lui en envoyer une copie.

En ce qui concerne le document du commissaire à la vie privée, c'était entièrement mon erreur. Je m'excuse au Comité. Malheureusement, cela m'a glissé des mains et n'a pas été produit aussi rapidement que je l'aurais voulu. Je demande l'indulgence du Comité à cet égard. Je vous présente mes excuses.

Merci.

Le président: Monsieur Lloyd, allez-y, puis nous passerons à M Caputo.

Dane Lloyd: Je vais peut-être céder la parole à M. Caputo.

Frank Caputo: Monsieur le président, je n'ai aucun problème à ce que M. Lloyd commence, car il était déjà sur une lancée.

Dane Lloyd: Merci.

Je remercie le greffier d'avoir fourni son explication. Nous savons que des accidents de la sorte se produisent.

On m'a dit que l'on pouvait accéder aux bleus à l'intérieur du pare-feu sur nos appareils. J'ai ici mon téléphone de la Chambre des communes. Je viens de regarder, et les bleus ne se trouvent pas sur mon téléphone de la Chambre des communes.

Vous savez, même si tout porte à croire qu'il s'agissait d'une erreur de bonne foi, compte tenu de la gravité du projet de loi dont nous sommes saisis, j'estime avoir été réellement désavantagé et que mon privilège a été enfreint de ne pas avoir eu accès à l'information correcte pour pouvoir participer pleinement à la séance. Je sollicite l'avis du président à ce sujet. Je crois que mon privilège a été enfreint.

Le président: Merci. Je tiendrai compte de votre commentaire et verrai avec le greffier — pas maintenant, mais tout de suite après la réunion — ce que nous pouvons faire, avec les commentaires de tout le monde, pour faciliter l'important travail à accomplir en une si courte période.

Afin que tout le monde le sache, vous disposez maintenant du document communiqué plus tôt par le commissaire. Nous pouvons utiliser ce document avec nos équipes pour aller de l'avant.

Encore une fois, je reviendrai sur cet aspect de l'atteinte au privilège, que vous avez d'ailleurs bien décrit.

Cela dit, monsieur Caputo, aimeriez-vous dire quelque chose avant de céder la parole à M. Lloyd pour ses cinq minutes?

● (1625)

Frank Caputo: Oui. Permettez-moi d'intervenir rapidement.

Compte tenu de ce que M. Lloyd a exprimé, à savoir que son privilège a été enfreint, et non pas seulement de manière prima facie, mais de façon manifeste, je vous demanderais, monsieur le président, si vous et le greffier pourriez vérifier la possibilité que le commissaire à la vie privée revienne la semaine prochaine et, en tout état de cause, avant l'étude article par article.

Je pense que la mesure corrective qui s'impose ici est de ne pas exiger le dépôt des amendements demain. Il me semble tout à fait évident qu'il s'agit de la seule solution possible dans un processus qui est déjà extrêmement précipité. À mon avis, cela illustre bien à quel point nous avançons trop rapidement. Je ne jette aucun blâme sur le greffier. Ce sont des choses qui arrivent. Des erreurs peuvent survenir. Nous avons eu des réunions de quatre heures, et nous sommes en plein milieu d'une autre séance de quatre heures.

Je m'arrête ici. Merci.

Le président: Sur ce, tout d'abord, nous avons un travail important à faire maintenant, alors je propose que nous nous y attaquions dès maintenant. Ensuite, comme je l'ai dit, j'examinerai la question de l'atteinte au privilège soulevée par le député Lloyd, et troisièmement, par la suite, nous chercherons ensemble — et avec vous en particulier, monsieur Caputo — à savoir comment la suggestion visant à changer l'horaire de l'étude du projet de loi pourrait être acceptée par les autres membres du Comité.

Frank Caputo: En fait, monsieur le président, j'ai des doutes. C'est quelque chose que j'envisageais de faire simultanément. Ne faut-il pas traiter sur-le-champ une question de privilège, à la première occasion possible? Je vous demande de bien vouloir consulter le greffier pour savoir si nous devons suspendre les travaux. Il est important de bien faire les choses, et non pas de les faire rapidement.

Le président: Les questions de privilège n'ont pas à être réglées maintenant par le président. Je peux demander l'indulgence du Comité pour y réfléchir — avec l'aide du greffier, évidemment, et d'autres personnes — après la réunion afin de décider comment aller de l'avant à partir de là. S'il s'agissait d'un rappel au Règlement, ce serait différent. Il s'agit d'une question de privilège, et je peux la prendre en considération après la séance.

Je conseillerais au Comité que nous procédions ainsi et que nous profitions de la présence des témoins pour faire avancer l'analyse du projet de loi à l'étude.

Cela dit, aimeriez-vous commencer votre intervention de cinq minutes, monsieur Lloyd?

Dane Lloyd: Dès que je… Oh, je suis désolé.

[*Français*]

Le président: Madame DeBellefeuille, vous avez la parole.

Claude DeBellefeuille: Monsieur le président, je voulais joindre ma voix au point important soulevé par M. Lloyd. J'attendais ce mémoire-là pour préparer des amendements. Je suis toujours impressionnée de voir que les recommandations du commissaire à la protection de la vie privée du Canada ne sont jamais prises en compte en amont de la rédaction. Je l'attendais avec impatience, parce que je savais que les délais étaient courts.

Je trouve pertinente la question de l'atteinte au privilège. Je pense qu'il faut vraiment regarder comment vous allez procéder. Nous souhaitons à la fois avoir le sentiment d'être capables de transmettre ces recommandations et d'avoir tenu compte de ce que le commissaire avait à dire.

Le président: Comme je l'ai dit en anglais, je vais prendre ça en considération. Ces informations auraient dû être disponibles il y a déjà quelque temps. Elles sont maintenant disponibles. Elles sont dans un format qui s'échelonne sur quatre pages. Comme le disait le commissaire, ces recommandations sont bien formulées. Elles sont claires, et elles peuvent être assez facilement comprises par les membres du Comité.

Cela étant dit, je propose au Comité que nous retournions à la comparution des témoins d'aujourd'hui. Je pourrai vous donner les points de vue et les recommandations des divers experts, y compris le greffier, après la rencontre.

Monsieur Lloyd, j'espère que ça vous va. Il faut poursuivre, sinon nous allons devoir passer à la séance suivante.

[*Traduction*]

Dane Lloyd: Je remercie les témoins.

Monsieur le commissaire Dufresne, nous avons reçu ici aujourd'hui un autre témoin qui a indiqué que le seuil des soupçons raisonnables pour les données de l'abonné lui semblait trop faible. Avez-vous des réflexions à ce sujet, ou cela dépasse-t-il votre champ de compétence?

Philippe Dufresne: Je pense qu'il est trop faible compte tenu de la formulation actuelle de la portée des renseignements relatifs à l'abonné: la définition et les parties qui peuvent les recevoir. Ma recommandation est de corriger la portée. Ainsi, vous pourrez garder le soupçon, mais si vous ne le faites pas, ce serait la solution de rechange.

Dane Lloyd: D'accord. Je vous remercie. Vous nous fournissez de nombreuses options ici.

Que pensez-vous des règles entourant la non-divulgation? Si une autorité s'adresse à un fournisseur de services électroniques pour obtenir des renseignements sur un abonné, elle peut imposer une clause de non-divulgation empêchant le fournisseur d'informer la personne visée qu'une communication a eu lieu. Qu'en pensez-vous?

● (1630)

Philippe Dufresne: Des raisons très valables pourraient justifier cette confidentialité. Le projet de loi comporte des améliorations pour ce qui est des rapports que le ministre doit présenter au Parlement et ainsi de suite.

L'une des lacunes que je recense dans mes huit recommandations, c'est que la confidentialité empêcherait le fournisseur d'aviser mon cabinet en cas d'atteinte et si des renseignements pertinents se trouvaient dans un arrêté ministériel. Il s'agit là à mon avis d'une lacune qui doit être comblée, car cela nous empêche de faire notre travail.

Dane Lloyd: Serait-il juste de dire que votre recommandation vise à ce que, chaque fois qu'une autorité demande des renseignements sur l'abonné, votre bureau soit avisé?

Philippe Dufresne: Pas nécessairement, mais je ne voudrais pas que la disposition sur la confidentialité empêche la communication d'information lorsque c'est approprié: avec mon bureau, par exemple, dans le cas d'une atteinte à la protection de la vie privée. C'est la situation la plus évidente.

Lorsqu'on aborde la question des renseignements relatifs à l'abonné et du chiffrement, la protection de l'information est absolument essentielle.

Dane Lloyd: Oui. Je pense qu'il y a certains cas où la non-divulgation est absolument nécessaire: par exemple, dans le cas d'enquêtes en cours. Croyez-vous que l'ajout de l'autorisation judiciaire au moment de solliciter une ordonnance de non-divulgation serait un moyen approprié de renforcer le régime?

Philippe Dufresne: Cela le renforce du point de vue de la protection de la vie privée. Il faudrait également tenir compte de l'impact sur le travail policier. Ce n'est pas l'une de mes huit recommandations prioritaires, mais c'est un élément à prendre en considération.

Dane Lloyd: C'est un compromis.

Philippe Dufresne: Je suppose que cela créerait des retards.

Dane Lloyd: D'accord. Merci.

En ce qui concerne les métadonnées, on a beaucoup parlé de l'exigence de conservation des métadonnées pour un an. Vous avez parlé de la « nécessité et de la proportionnalité ». Est-il nécessaire et proportionnel de conserver les métadonnées de tous les Canadiens pour une période pouvant aller jusqu'à un an?

Philippe Dufresne: Je pense que la condition de la nécessité et de la proportionnalité doit exister dès que vous exercez ce pouvoir, qu'il s'agisse du Cabinet pour ce qui est des ordonnances ou du ministre. Avec ce cadre, on traite la question au cas par cas. Il peut y avoir des situations où la gravité et l'importance sont telles qu'il peut y avoir des justifications; ce serait alors au gouvernement ou aux services policiers de les fournir. Je ne veux pas préjuger de ces situations. Sans ce cadre, toutefois, on risque d'avoir des ordonnances trop longues et trop larges. C'est pourquoi la nécessité et la proportionnalité sont des éléments fondamentaux du droit à la vie privée.

Dane Lloyd: Vous préoccupez-vous des répercussions sur la vie privée du fait d'obliger les entreprises à conserver les métadonnées des Canadiens pendant un an?

Philippe Dufresne: Plus vous conservez les renseignements longtemps, plus il existe un risque en matière d'atteinte à la vie privée, et plus il y a des répercussions en cas d'atteinte. L'un des principes que nous préconisons est de ne pas conserver les renseignements plus longtemps que nécessaire. Encore une fois, c'est pourquoi la nécessité et la proportionnalité sont aussi importantes. Il arrivera parfois que vous deviez les garder plus longtemps, mais cela doit être vérifié dans chaque cas.

Dane Lloyd: Nous avons entendu parler de vulnérabilité systémique. Le gouvernement a affirmé qu'il n'introduira pas de vulnérabilités systémiques. Cependant, il semble que, en vertu des arrêtés ministériels, il pourrait très bien ordonner aux entreprises d'installer des éléments qui créeraient des vulnérabilités.

Qu'en pensez-vous?

Philippe Dufresne: Je sais qu'on a débattu à ce sujet. Le projet de loi comporte maintenant une définition de « vulnérabilité systémique ». Je pense avoir entendu des représentants gouvernementaux dire qu'ils n'ont pas l'intention de l'affaiblir.

Ce que je propose, c'est que cela soit clair dans le projet de loi. Il existe un modèle pour ce type de choses en Australie, où…

Dane Lloyd: Je suis désolé.

Pour terminer, monsieur Lefebvre, j'ai entendu un électeur qui s'est présenté à mon bureau la semaine dernière exprimer sa préoccupation selon laquelle, si nous créons des portes dérobées potentielles, ce qui pourrait assurément être fait dans le cadre du projet de loi — peut-être pas dès maintenant —, des renseignements préjudiciables au sujet des personnes pourraient être fabriqués et ajoutés à leurs comptes pour les faire paraître coupables.

Est-ce une tactique utilisée par les extorqueurs? Pourraient-ils exploiter les avances en matière de chiffrement pour le faire?

Luc Lefebvre: S'il existe une porte dérobée, elle peut essentiellement être utilisée par qui que ce soit, même les personnes qui ne sont pas censées l'utiliser.

Il est certain que, une fois que vous avez accès aux données, vous pouvez les manipuler de toutes les façons possibles. C'est évidemment un élément que des acteurs malveillants, des criminels ou des adversaires pourraient utiliser pour fabriquer une allégation à propos de quelqu'un.

[*Français*]

Le président: Merci beaucoup, monsieur Lloyd.

Je passe maintenant la parole à M. Ramsay pour cinq minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Monsieur Lefebvre, est-ce que les métadonnées sont cryptées?

Luc Lefebvre: Ça dépend, il y a des...

Jacques Ramsay: Je pense que non.

Luc Lefebvre: En fait, certaines métadonnées sont cryptées, selon les systèmes. L'application Signal en est un magnifique exemple.

Dans cette application, les métadonnées sont cryptées. Certaines données ne sont pas cryptées, comme la date de création du compte et de la dernière connexion. Toutefois, une fois que la personne est connectée à l'application Signal dans son compte, on ne peut pas savoir qui communique avec qui, à quel moment, les titres des discussions qu'ils ont eues, contrairement, par exemple, à un courriel.

Dans une application de courriel, on peut avoir accès à certaines informations: qui a parlé à qui, quand, le serveur par lequel le courriel est passé, le titre du courriel. Nous ne verrons pas nécessairement le contenu du courriel, mais nous pourrons avoir accès à ces métadonnées. Ça dépend donc du type de système, du type de chiffrement qui est utilisé par l'application.

Dans le cas présent, l'objectif est de diminuer le chiffrement pour que nous puissions avoir accès à certaines données auxquelles nous n'avions pas accès auparavant, comme dans l'application Signal.

● (1635)

Jacques Ramsay: D'accord, j'accepte votre définition, monsieur Lefebvre. La compagnie Signal se distingue par le secret avec lequel elle entoure ses métadonnées.

La plupart du temps, sauf erreur, les messages sont cryptés, et le gouvernement a bien précisé qu'il ne voulait rien savoir des messages. Nous parlons de données comme les dates ou les lieux. Il n'y a rien de crypté là-dedans. Le gouvernement n'est pas dans une mission de décryptage des envois.

Monsieur Dufresne, vous nous dites que le gouvernement est là pour faire la chasse aux méchants. Nous ne sommes pas là pour aller voir des rapports de santé. Nous ne sommes pas là pour ça.

Étant donné que nous, comme nos collègues d'en face, n'avons pas eu accès à votre rapport, pouvez-vous nous dire quelle est la principale recommandation qui fera en sorte que la loi va se limiter à aller chercher les informations qui sont de nature criminelle?

Philippe Dufresne: Je pense que ce sont les recommandations 1, 2 et 3 dans mon mémoire.

Il s'agit d'être plus précis sur le type d'information qui peut être obtenue. Je pense que c'est l'intention du gouvernement, donc le fait de le préciser va rassurer les gens qui sont inquiets par rapport à ça.

Il s'agit aussi de préciser les types d'individus et d'organisations qui peuvent recevoir ces demandes. En ce moment, il est question de fournisseurs de services au public. C'est large. Ça peut inclure des renseignements de nature médicale, par exemple.

À mon avis, ça devrait être des fournisseurs de services de télécommunications, comme c'est le cas pour les articles précédents, qui traitent des demandes sans mandat. Je pense que ça viendrait restreindre l'accès à ce qui est véritablement l'objectif du projet de loi.

Jacques Ramsay: D'accord. Merci.

J'aimerais que les gens du Barreau du Québec m'aident. Je ne suis pas avocat, mais vous représentez également les procureurs, qui sont aussi des avocats.

N'est-ce pas?

Marcel-Olivier Nadeau: Je ne dirais pas que nous les représentons, monsieur Ramsay, mais ils sont en effet membres...

Jacques Ramsay: Ils doivent être membres, car ils paient une cotisation.

Marcel-Olivier Nadeau: Absolument.

Jacques Ramsay: Ont-ils donc été consultés dans le cadre de l'élaboration de votre mémoire?

Marcel-Olivier Nadeau: Oui.

Nous consultons un comité d'experts en droit criminel constitué pour la moitié de criminalistes et pour la moitié de poursuivants.

Jacques Ramsay: D'accord.

Vous nous avez parlé du « motif raisonnable de soupçonner » par opposition au « motif raisonnable de croire ».

Évidemment, personne n'est contre la vertu. Tout le monde aimerait avoir un plus haut standard. Toutefois, la prémisse du gouvernement est de dire que les informations que nous allons chercher, c'est-à-dire ces métadonnées, ne sont pas des éléments de preuve pouvant être présentés en cour. Ce sont des informations qui aideront à faire avancer une enquête afin d'aller chercher des preuves qui pourraient finir par être utilisées en cour. C'est pour ça que le gouvernement parle de « motif raisonnable de soupçonner » plutôt que de « motif raisonnable de croire ». C'est quand même une norme juridique acceptable, bien connue et reconnue.

Marcel-Olivier Nadeau: Sur cet aspect, je vais laisser M^{e} Marchand répondre.

Michel Marchand: Nous trouvons que les soupçons représentent une norme trop basse. Quand on lit le jugement qui a été rendu par la Cour suprême dans l'arrêt Bykovets, on voit qu'on y souligne l'ampleur de l'atteinte à la vie privée que permet l'accès à l'adresse IP. L'accès à l'adresse IP donne accès à tout.

Selon la façon dont le projet de loi est libellé actuellement, si on confirmait la fourniture de services sur la base des soupçons, ce serait tout simplement parce que les renseignements obtenus pourraient être utiles à l'enquête. Ce n'est pas parce qu'un suspect aurait commis une infraction, mais bien parce que les renseignements seraient utiles à l'enquête.

Dans le jugement maître en matière de soupçons raisonnables, on dit qu'un tel critère cible aussi beaucoup de personnes qui n'ont rien à voir dans l'histoire.

On est alors rendu...

● (1640)

Jacques Ramsay: Vous avez le deuxième critère, qui est précisément la raison pour laquelle l'information va être utile à l'enquête, et...

Le président: Je suis désolé de vous couper la parole...

Jacques Ramsay: Je ne suis pas d'accord avec vous quand vous dites que ça donne accès à tout. Ce n'est pas vrai.

Le président: Monsieur Ramsay, je suis désolé de vous couper la parole. Je dois passer à Mme...

[*Traduction*]

Frank Caputo: J'ai un rappel au Règlement, s'il vous plaît.

Pendant un instant, j'ai cru qu'il n'y avait que moi, le ministre, M. Ramsay et notre témoin, mais mon rappel au Règlement porte sur la question de privilège soulevée par M. Lloyd.

J'ai parlé avec le greffier. J'inviterais le greffier à confirmer aux fins du compte rendu et je vous inviterais vous, monsieur le président, à confirmer pour le compte rendu que vous n'avez pas vu le mémoire du commissaire à la vie privée et que le greffier, à sa connaissance, ne vous l'a pas communiqué.

Est-il exact, monsieur le président, que vous n'avez pas vu le mémoire du commissaire à la vie privée?

Le président: Je vous remercie de votre question, monsieur Caputo. Comme je l'ai dit précédemment, cette question de privilège mérite qu'on y accorde toute l'attention voulue. Mon attention porte maintenant sur le fait de permettre aux témoins de tirer le meilleur parti de leur temps et de leurs contributions. Si vous le permettez, je me pencherai sur la question après la réunion et étudierai cette question de privilège de la manière appropriée.

Frank Caputo: Avec tout le respect que je vous dois, monsieur le président, nous devons décider maintenant comment procéder.

Si vous avez reçu ce mémoire ou ne l'avez pas reçu, cela a des répercussions sur certaines choses. Tout ce que je vous demande, monsieur le président, c'est de me dire si oui ou non vous aviez vu le mémoire du commissaire à la vie privée.

Le président: Pour autant que je sache, je n'ai pas vu ce courriel, mais j'aimerais faire une vérification et m'assurer que je fournis aux membres du Comité l'information la plus exacte.

Frank Caputo: Merci.

Le président: Cela étant dit, nous passons à Mme DeBellefeuille.

[*Français*]

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

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur le bâtonnier, je vais demander à M. Marchand de continuer sur la lancée des réponses qu'il a données à notre secrétaire parlementaire.

Au fond, si j'ai bien compris, les « motifs raisonnables de soupçonner » auxquels renvoie le projet de loi C-22 sont utilisés pour des données particulières, qui ne sont pas jugées sensibles.

De votre côté, vous défendez le contraire. Alors que le ministère de la Justice, le ministre de la Justice et le personnel du ministère disent que ça respecte le jugement de la Cour suprême, vous ne semblez pas être du même avis.

Pourriez-vous poursuivre votre analyse pour que nous puissions vraiment bien vous comprendre à ce sujet?

Michel Marchand: De notre côté, nous pensons que ça ne respecte pas du tout le jugement de la Cour suprême. Le nouvel article 487.0142 du Code criminel qui est proposé est très large. On y parle notamment de « tous les renseignements relatifs à l'abonné [...], notamment des données de transmission ». L'adresse IP permet donc de couvrir tout ça. De plus, si on lit correctement et attentivement le jugement de la Cour suprême rendu il n'y a quand même pas si longtemps, on voit dans l'arrêt Bykovets que les juges majoritaires ont dit que l'adresse IP était comme une clé de voûte.

Les choses ne se passent plus comme avant, quand on faisait une perquisition. Auparavant, quand des policiers faisaient une perquisition, ils arrivaient dans une maison et y trouvaient quelque chose ou non. Maintenant, avec l'adresse IP, on a accès à presque toute la vie d'une personne. On peut trouver le dossier médical de la personne, ce dont elle rêve, ce qu'elle a écrit sur Internet et une foule d'autres renseignements. De plus, on nous dit que les données obtenues seraient conservées pendant un an. C'est donc comme si on donnait accès à une grande banque de données où l'on peut espionner ou essayer de trouver tout ce que l'on veut.

Claude DeBellefeuille: Merci, monsieur Marchand. Je pense que j'ai bien compris votre idée. Vous êtes quand même expert du Barreau du Québec. On pourrait douter d'un tel témoignage de la part de quelqu'un qui doute de tout, mais votre témoignage est très crédible, selon moi.

J'essaie de voir comment on peut améliorer le projet de loi. Donc, vous nous conseillez de supprimer le seuil du « motif raisonnable de soupçonner ».

De son côté, le commissaire nous recommande de restreindre l'utilisation de ce seuil.

C'est ce que j'ai compris de vos recommandations, monsieur Dufresne.

Philippe Dufresne: Tout à fait. Vous avez les deux options.

Claude DeBellefeuille: Pour terminer, je voudrais vous remercier.

Le président: Madame DeBellefeuille, il faudrait vraiment terminer, parce que votre temps de parole est écoulé.

Claude DeBellefeuille: Merci.

Vous voyez comme il est poli avec moi.

Le président: Vous me désolez en me disant des mots aussi durs.

Je remercie tous les témoins d'avoir pris le temps de se préparer à la réunion et de se déplacer ou de participer par vidéoconférence.

Nous n'aurons pas beaucoup l'occasion de vous saluer chaleureusement après votre départ, parce que nous devons commencer la deuxième partie de la réunion. Alors, nous vous invitons à passer une bonne fin de journée. Merci.

● (1645)

_____(Pause)_____

● (1649)

● (1645)

Le président: Bonjour, tout le monde.

Nous commençons la deuxième partie de cette réunion avec de nouveaux témoins, auxquels j'aimerais souhaiter la bienvenue.

Nous recevons, de la compagnie Apple, Erik Neuenschwander, directeur principal, Confidentialité des utilisateurs et de la sécurité des enfants.

De l'Association canadienne des libertés civiles, nous recevons Tamir Israel, directeur, Programme sur la protection de la vie privée, de la surveillance et de la technologie. Il participe à la réunion par vidéoconférence.

De Google, nous recevons Katherine Charlet, directrice principale, et Jeanette Patell, directrice, Affaires gouvernementales et politiques publiques, qui participent toutes les deux par vidéoconférence.

Nous allons commencer les présentations de cinq minutes.

Monsieur Neuenschwander, vous avez la parole.

● (1650)

[*Traduction*]

Erik Neuenschwander (directeur principal, Confidentialité des utilisateurs et de la sécurité des enfants, Apple Inc.): Merci.

Bonjour, monsieur le président, madame et monsieur les vice-présidents et mesdames et messieurs. Je m'appelle Erik Neuenschwander et je suis directeur principal des utilisateurs et de la sécurité des enfants chez Apple, où je travaille comme ingénieur logiciel depuis 19 ans. J'ai été le premier ingénieur en analyse de données sur le premier iPhone, et j'ai fondé l'équipe d'ingénierie de la protection de la vie privée chez Apple. Aujourd'hui, mon travail consiste à m'assurer que les produits et services d'Apple protègent les renseignements de nos utilisateurs. Merci de m'avoir invité à prendre la parole devant vous aujourd'hui.

Comme vous le savez, il se pourrait que ce soit l'une des dernières fois où nous sommes autorisés à discuter publiquement des conséquences de ce projet de loi. C'est le résultat des clauses de secret prévues dans le projet de loi, qui empêchent les entreprises comme Apple d'informer leurs utilisateurs ou le public des ordonnances reçues.

Alors, aujourd'hui, je veux être clair au sujet de notre approche de la vie privée chez Apple. Et je veux être clair concernant les raisons pour lesquelles le chiffrement est si important pour défendre la vie privée et la sécurité des gens au Canada et partout dans le monde.

Ces enjeux n'ont jamais été aussi importants, parce que notre monde devient de plus en plus numérique. En tant qu'utilisateurs, nous comptons sur notre technologie pour stocker et traiter de façon sécurisée des données très sensibles, comme nos données de santé, nos photos et la localisation de nos proches. Les endroits où nous conservons notre argent, stockons nos fichiers et faisons des affaires sont de plus en plus en ligne, et parfois uniquement en ligne. Et les infrastructures essentielles que nous tenons souvent pour acquises — du réseau électrique aux réseaux de transport — dépendent de plus en plus d'appareils connectés.

Mais à mesure que la technologie évolue, les acteurs malveillants qui cherchent à voler nos données évoluent eux aussi. Le Canada l'a vécu directement. En 2023, il figurait parmi les pays les plus fréquemment ciblés par des attaques de rançongiciels. L'an dernier encore, des acteurs malveillants ont visé des entreprises de télécommunications canadiennes et d'autres réseaux dans le cadre de la vaste attaque Salt Typhoon, non seulement pour voler des données de clients, mais aussi pour mener de l'espionnage à grande échelle et prendre le contrôle des infrastructures de communication dont des milliards de personnes dépendent chaque jour.

En tant qu'entreprise technologique, Apple travaille constamment à anticiper et à prévenir ces menaces. Et en tant qu'ingénieur, je peux vous dire que le chiffrement de bout en bout est l'une des technologies de sécurité les plus efficaces pour s'en défendre. Le chiffrement protège les Canadiens contre le vol d'identité, la fraude, la surveillance illégale et les fuites de données. Il protège les infrastructures essentielles. Et il protège les données et les communications sur lesquelles les entreprises et le gouvernement canadiens s'appuient, ce qui est crucial pour la réussite économique et la sécurité nationale du Canada.

Nos utilisateurs font confiance aux appareils Apple pour leurs renseignements les plus sensibles. Ils s'attendent à bénéficier des protections les plus robustes, et ils les méritent. C'est pourquoi nous sommes si préoccupés par la menace que le projet de loi C-22 fait peser sur le chiffrement. Tel qu'il est actuellement rédigé, le projet de loi permettrait au gouvernement du Canada de forcer les entreprises à contourner le chiffrement en y intégrant des portes dérobées, quelque chose qu'Apple ne fera jamais.

Je tiens à préciser que nous partageons l'engagement du gouvernement envers la sécurité de tous les Canadiens. Nous disposons d'une équipe de professionnels dévoués, disponibles vingt-quatre heures sur vingt-quatre pour aider les forces de l'ordre. Entre 2020 et 2024 seulement, nous avons reçu un peu plus de 3 200 demandes de renseignements de la part du gouvernement canadien, dont environ 35 % étaient des demandes urgentes. Nous sommes déterminés à soutenir le travail des forces de l'ordre pour assurer la sécurité des Canadiens. Et nous sommes déterminés à défendre le chiffrement pour la même raison… parce qu'il assure la sécurité des Canadiens.

Je le répète — en tant qu'ingénieur, je ne connais aucune façon de déployer une technologie de chiffrement qui n'offrirait l'accès qu'aux bonnes personnes sans créer de nouvelles façons pour les mauvaises d'entrer. Autrement dit, quand on construit une porte dérobée dans un appareil chiffré, n'importe qui peut la franchir. Et parce que tant de choses reposent sur le chiffrement, nous ne pouvons pas prendre ce risque.

Il suffit de regarder l'attaque Salt Typhoon. Les États-Unis ont adopté une loi obligeant les entreprises de télécommunications à intégrer des points d'accès pour les forces de l'ordre dans leurs systèmes, et des acteurs parrainés par des États les ont ensuite exploités. Cette loi allait moins loin que le projet de loi C-22. Imaginez alors ce qui pourrait se passer si davantage d'entreprises étaient tenues de créer ces vulnérabilités.

Apple a déposé un mémoire proposant des amendements ciblés qui amélioreraient le projet de loi, et je serai heureux d'en discuter. Nous appelons particulièrement le Comité à adopter des amendements qui interdiraient explicitement toute exigence qui affaiblirait, contournerait ou compromettrait le chiffrement de bout en bout. Nous croyons que ces modifications permettraient tout de même d'élargir l'accès légal, et de doter les forces de l'ordre canadiennes de nouveaux outils pour lutter contre la criminalité au 21e siècle.

Encore une fois, merci de m'avoir donné l'occasion de prendre la parole aujourd'hui. Je suis à votre disposition pour répondre à vos questions.

● (1655)

Le président: Merci beaucoup.

Nous cédons maintenant la parole à Tamir Israel pour cinq minutes, s'il vous plaît.

Tamir Israel (directeur, Programme de la protection de la vie privée, de la surveillance et de la technologie, Association canadienne des libertés civiles): Monsieur le président et honorables membres du Comité, bonjour. Je vous remercie de m'avoir invité aujourd'hui à m'adresser à vous concernant le projet de loi C-22, Loi concernant l'accès légal.

La partie 1 du projet de loi C-22 représente une amélioration considérable par rapport à celui qui l'a précédé; cependant, certains éléments de la partie 1 continuent de souffrir d'une portée excessive. Cela comprend l'utilisation de normes faibles concernant l'accès autorisé par l'appareil judiciaire à des données sensibles sur l'abonné et un cadre qui invite la collecte inconstitutionnelle de données publiquement accessibles.

Certains éléments de la partie 1 permettent également au Canada d'adopter au moins un, voire deux accords internationaux d'échange de renseignements, malgré une tendance croissante à utiliser ces instruments pour la répression transfrontalière et en l'absence de garanties comparables.

L'ACLC dépose un mémoire conjoint avec Kate Robertson et Cynthia Khoo du Citizen Lab, qui approfondira ces éléments ainsi que d'autres aspects problématiques du projet de loi C-22. Pour le reste de mes commentaires cet après-midi, je me concentrerai sur la partie 2 du projet de loi, qui édicterait la Loi sur l'accès autorisé à l'information, ou LSAAI.

À divers moments, les gouvernements ont cherché à élargir leurs capacités de surveillance aux dépens de la cybersécurité, le chiffrement étant une cible récurrente. Trop souvent, ces expansions ont été justifiées par l'attente selon laquelle les capacités de surveillance ne seront utilisées que par des agences gouvernementales autorisées par la loi et non pas par des acteurs malveillants, or encore et encore, cette attente s'est révélée fausse. L'attaque Salt Typhoon est le dernier et peut-être le plus puissant rappel de cette dure leçon.

Il convient également de noter que la justification de cette disposition législative n'a pas été démontrée. En fait, la moitié de nos partenaires du Groupe des cinq a limité ses régimes de capacité de surveillance à l'imposition d'obligations en matière d'écoute électronique pour les entreprises de télécommunications. Compte tenu d'un historique préoccupant, la LSAAI présente trois lacunes fondamentales, étroitement liées entre elles.

Premièrement, la LSAAI est excessivement large. Elle s'applique à tout fournisseur de tout service qui détient une composante numérique. En vertu de la version australienne de cette loi, tout ce qui va d'une chaîne d'alimentation rapide qui fournit le service sans fil à ses clients au magasin d'électronique qui entretient les téléphones et les ordinateurs des clients, jusqu'au détaillant qui possède une application de téléphone mobile ou un site Web, a été considéré comme une cible.

La LSAAI est également vaste en ce qui concerne les obligations que le gouvernement peut imposer. Cela va du fait d'exiger la capacité de réinitialiser secrètement les mots de passe des clients ou d'imposer un outil automatique qui génère des profils clandestins réalistes sur les plateformes de médias sociaux jusqu'au fait d'exiger la capacité de bloquer l'utilisation par une cible de services de messagerie privée chiffrée afin de la forcer à utiliser des solutions de rechange peu sécuritaires.

Le mécanisme de conservation des métadonnées de la LSAAI est, lui aussi, large. Les services pourraient être tenus de conserver un dossier détaillé des déplacements de chaque personne, de ses interactions interpersonnelles, des applications qu'elle utilise et plus encore. Il s'agit de données hautement sensibles.

Deuxièmement, le maintien des limites et des garanties ne parvient pas à encadrer les multiples façons dont la vie privée, le chiffrement et d'autres protections des données pourraient être compromis, compte tenu de la portée étendue du projet de loi. La limite de la vulnérabilité systémique, prévue dans la LSAAI, par exemple, ne s'appliquerait pas à un ensemble d'outils de surveillance algorithmique connus sous le nom d'analyse côté client. Puisque ces outils contournent le chiffrement plutôt que de le compromettre directement, ils ne sont pas visés par la limite de la vulnérabilité systémique telle qu'elle est rédigée. Ils créent néanmoins une vulnérabilité systémique en pratique.

Troisièmement, bien que les tribunaux demeurent le principal mécanisme d'autorisation des activités de surveillance du SCRS et des services policiers, la LSAAI ne repose pas sur une autorisation judiciaire, alors même qu'elle confère des pouvoirs dont la portée rivalise fréquemment avec leurs équivalents prévus dans le Code criminel. Par exemple, si les services policiers veulent forcer une entreprise à conserver les métadonnées d'un client particulier pendant 90 jours, ils ont besoin d'une ordonnance du tribunal, mais pour forcer la même entreprise à conserver les mêmes métadonnées pour chaque client pendant une période pouvant aller jusqu'à un an, le gouvernement n'a qu'à imposer une obligation en vertu de la LSAAI. Le contrôle judiciaire est disponible et même requis dans certains cas, mais celui-ci s'en remet principalement aux décisions du gouvernement et ne remplace pas une autorisation indépendante, un examen *de novo* ou le plein droit d'appel. C'est le cas tout particulièrement lorsqu'un grand nombre des obligations sont imposées en secret, comme c'est le cas en vertu de la LSAAI.

En résumé, la LSAAI présente une menace importante à la vie privée et à la cybersécurité. Il n'est pas clair comment les nombreuses lacunes qui se recoupent au sein de la LSAAI pourraient être corrigées dans le cadre de l'étude législative extrêmement limitée dont elle fait l'objet. Le régime de capacités techniques de l'Australie a été modifié 173 fois lors d'une étude détaillée en comité. Malgré ces modifications, elles ont tout de même été jugées vraisemblablement incompatibles avec les droits de la personne, ce qui a entraîné l'obligation de procéder à une évaluation obligatoire de la mesure législative.

Nous vous pressons donc de recommander au gouvernement de faire avancer le projet de loi C-22 sans la partie 2. Ce projet de loi sera en vigueur pour les années à venir, et il est extrêmement important de bien le rédiger. Les enjeux sont tout simplement trop élevés.

Je vous remercie. J'ai terminé ma déclaration liminaire. Je répondrai volontiers à vos questions.

● (1700)

[*Français*]

Le président: Merci, monsieur Israel.

Je passe maintenant la parole à Mme Jeanette Patell pour cinq minutes.

[*Traduction*]

Jeanette Patell (directrice, Affaires gouvernementales et des politiques publiques, Canada, Google): Bonjour, monsieur le président, madame et monsieur les vice-présidents et mesdames et messieurs.

Je m'appelle Jeanette Patell. Je suis directrice des Affaires gouvernementales et des politiques publiques pour Google Canada. Je suis accompagnée aujourd'hui par Kate Charlet, directrice principale de l'équipe de politiques publiques de Google, où elle dirige nos travaux sur la cybersécurité, la protection de la vie privée et la sécurité des enfants. Avant de se joindre à Google, elle a occupé pendant dix ans des fonctions de sécurité nationale au Pentagone et à la Maison-Blanche.

Google s'engage à soutenir les efforts des forces de l'ordre en protégeant le public contre les crimes et le terrorisme. Nous croyons fermement que l'amélioration de la sécurité du public et que le maintien de la sécurité des utilisateurs sont des objectifs très compatibles.

En tant que chef de file mondial dans la conception de produits sûrs et sécuritaires, nous prenons très au sérieux la vie privée et la sécurité de nos utilisateurs. Notre modèle d'affaires repose sur la confiance que nos utilisateurs nous accordent pour assurer la sécurité de leurs données. Les produits Google sont privés et sécurisés par conception, protégés par de nombreuses couches de sécurité et de technologies de pointe, comme le chiffrement.

Je tiens à être absolument claire: Google n'a jamais conçu de porte dérobée ni tout autre mécanisme visant à contourner le chiffrement de bout en bout de ses produits. Lorsque nous affirmons qu'un produit est chiffré de bout en bout, il l'est.

Dans l'environnement de menaces qui évolue rapidement d'aujourd'hui, nous croyons qu'il est essentiel de trouver des moyens de soutenir l'important travail des forces de l'ordre sans intégrer dans nos produits et nos services des vulnérabilités qui affaiblissent la sécurité pour tous.

Dans ce contexte, Google a d'importantes préoccupations concernant plusieurs éléments de la partie 2 du projet de loi C-22 tel qu'il est actuellement rédigé.

Premièrement, le régime proposé envisage des obligations et des pouvoirs de rendre des ordonnances qui sont indûment vastes et pratiquement illimités. Cela va bien au-delà des régimes d'accès légal d'autres démocraties du G7 et risque de créer une nouvelle infrastructure de surveillance qui introduirait des vulnérabilités de sécurité graves, minerait la confiance des utilisateurs et nuirait à notre capacité d'innover et d'offrir des technologies favorables à la protection de la vie privée.

Deuxièmement, le cadre proposé concernant les arrêtés ministériels secrets n'a aucun précédent et mine la responsabilisation et la confiance des utilisateurs. La partie 2 confère au ministre de la Sécurité publique de vastes pouvoirs d'émettre des ordonnances secrètes obligeant les fournisseurs à créer ou à maintenir des capacités d'interception de données, tout en interdisant de façon permanente aux entreprises de divulguer l'existence de ces ordonnances. Tel qu'il est rédigé, cela fournirait au gouvernement le pouvoir de forcer secrètement des entreprises à reconcevoir leurs produits pour inclure des capacités de surveillance invasives, et ce, sans mesures de protection ou surveillance suffisantes.

Les arrêtés ministériels sont non seulement alarmants, mais aussi inutiles. Le Canada dispose déjà d'un système efficace et transparent qui permet aux forces de l'ordre de demander aux tribunaux des ordonnances d'assistance raisonnable assujetties à une surveillance judiciaire. Les ordonnances secrètes constituent une mesure déphasée par rapport à d'autres pays démocratiques et limiteraient grandement la capacité des entreprises de communiquer de façon transparente aux utilisateurs la façon dont leurs données sont protégées.

Troisièmement, la définition de « vulnérabilité systémique » inscrite dans le projet de loi est très étroite, ce qui est dangereux. Le projet de loi fixe la barre très haut, reconnaissant uniquement comme vulnérabilité le « risque sérieux » d'accès non autorisé, tout en faisant fi de risques graves pour l'intégrité et la disponibilité des données. La définition actuelle ne parvient pas à protéger explicitement les mesures de sécurité globales sur lesquelles les Canadiens comptent, qui vont bien au-delà du chiffrement.

Sans définitions plus solides, la loi pourrait être utilisée pour forcer le démantèlement de l'architecture essentielle en matière de vie privée, notamment en perçant le chiffrement, en contournant les contrôles de suppression des données des utilisateurs ou en intégrant une capacité d'accès à distance, toutes ces mesures facilitant l'ingérence étrangère et affaiblissant la protection globale de la vie privée des utilisateurs. À un moment où les cybermenaces sont de plus en plus fréquentes et perfectionnées et où les acteurs malveillants utilisent des outils d'intelligence artificielle pour repérer et exploiter plus rapidement les vulnérabilités, nous ne pouvons nous permettre d'en créer de nouvelles.

[*Français*]

Enfin, le projet de loi impose des exigences trop vastes en matière de conservation des métadonnées, sans aucun critère géographique, temporel ou ciblé. De telles exigences rendraient obligatoire la conservation générale et sans distinction des données de communication des gens et risqueraient de traiter l'ensemble de la population comme des suspects potentiels.

La conservation inutile des données menace les libertés et les droits fondamentaux des Canadiennes et des Canadiens, porte atteinte à leur vie privée et crée une mine massive de données sensibles qui amplifie les conséquences de toute atteinte potentielle à la sécurité. Les dispositions existantes pour les ordonnances de conservation ciblées dans le Code criminel répondent déjà aux besoins d'application de la loi, tout en respectant les droits garantis par la Charte.

[*Traduction*]

Pour faire en sorte que le projet de loi C-22 atteigne ses objectifs en matière de sécurité publique sans compromettre la sécurité numérique des Canadiens, Google a présenté un certain nombre d'amendements législatifs. Nous serons heureuses d'en discuter aujourd'hui.

Merci de nous avoir fourni l'occasion de contribuer à ce processus. Je répondrai volontiers à vos questions.

● (1705)

[*Français*]

Le président: Merci beaucoup, madame Patell.

Monsieur Caputo, vous avez la parole pour six minutes.

[*Traduction*]

Frank Caputo: Merci beaucoup, monsieur le président.

Monsieur Neuenschwander, tout d'abord, merci d'être ici et merci aux témoins. Il est rare de recevoir ici un ingénieur qui possède vos qualifications. Nous pourrions passer toute l'heure avec vous.

Avez-vous suivi le processus du Comité concernant ce projet de loi, si je peux poser la question?

Erik Neuenschwander: L'équipe l'a fait. Nous avons été tenus au courant. J'étais ici au cours de l'heure précédente.

Frank Caputo: Je serai très direct. Je pense que ce dossier a été très précipité. Il y a beaucoup de questions auxquelles on doit répondre et d'éléments à régler. Êtes-vous du même avis?

Erik Neuenschwander: Nous sommes ici pour collaborer avec le Comité, quel que soit le temps dont il dispose.

Frank Caputo: Serait-ce utile si le Comité avait plus de temps pour discuter du projet de loi, selon vous?

Erik Neuenschwander: Encore une fois, je suis simplement heureux d'être ici et de répondre à des questions, comme nous le ferons.

Frank Caputo: Monsieur Israel, puis-je vous poser la même question, s'il vous plaît?

Tamir Israel: Il serait certainement utile d'avoir plus de temps. Le Comité a eu trois jours de séance pour entendre des témoins. Ce n'est pas suffisant pour un projet de loi de ce niveau de complexité.

J'ai mentionné l'examen dont la version australienne de ce projet de loi a fait l'objet. Il était beaucoup plus exhaustif. Ce Comité a étudié le projet de loi C-8 pendant peut-être deux mois, et il s'agit d'un régime similaire qui soulève des questions similaires, mais de complexité et de portée moindres. Je dirais donc oui; il faut plus de temps pour étudier le projet de loi.

Frank Caputo: Oui, je pense que ce projet de loi est beaucoup plus technique que le projet de loi C-8 parce que, avec celui-là, nous arrivions à comprendre ce que signifiaient les différents éléments. Je pense que nous recevrons un témoin dans le prochain groupe qui viendra en fait exposer ce que sont les métadonnées.

Nous ne sommes pas réellement entrés dans les aspects techniques. Nous avons essentiellement entendu des gens comme vous — des gens de Google, d'Apple — exprimer leurs préoccupations, mais nous n'avons pas eu le temps de nous pencher sur les aspects techniques en ce qui concerne ce que signifie le chiffrement. Est-ce le cas pour tous les aspects? Est-ce pour le chiffrement de bout en bout? Je ne suis pas expert dans ce domaine, et nous n'avons pas entendu d'experts s'exprimer sur ces données ou cette analyse. Cela me préoccupe fortement.

Monsieur Neuenschwander et madame Patell, vous pouvez intervenir à ce sujet. Le ministre n'a pas répondu clairement lorsque je l'ai questionné sur le chiffrement. Même si, en tant que conservateurs, nous allons proposer des amendements qui indiqueront clairement que le chiffrement sera écarté lorsque le projet de loi fera l'objet de l'étude article par article, êtes-vous toujours préoccupé par le fait qu'il touche aux technologies de chiffrement?

Erik Neuenschwander: Nous aimerions bien voir cet amendement, mais nous avons des préoccupations qui dépassent le chiffrement en ce qui concerne la manière dont le risque est évalué. Étant donné qu'un chiffrement solide protège tous les utilisateurs de nos services, pas seulement ceux d'Apple, mais de l'ensemble de l'industrie, nous jugeons crucial que cela demeure protégé à mesure que le projet de loi C-22 va de l'avant.

Frank Caputo: Madame Patell, souhaitez-vous ajouter quelque chose?

Jeanette Patell: Oui. Dans le même ordre d'idées, nous avons proposé un certain nombre de recommandations concernant la manière de renforcer le projet de loi. Je pense que le chiffrement est un aspect dont nous pourrions parler, mais comme Apple, il nous semble que la définition de « vulnérabilité systémique » est un domaine qui pourrait être renforcé, ainsi que les vastes arrêtés ministériels.

Je sais que ma collègue, Mme Charlet, serait heureuse de nous expliquer davantage comment cet aspect pourrait être renforcé afin d'être davantage conforme aux normes internationales [*difficultés techniques*].

Frank Caputo: Je vais poser une question à ce sujet. L'un des problèmes que je vois ici, c'est que le gouvernement a essayé d'instaurer un système de freins et de contrepoids sous la forme d'une approbation par le commissaire au renseignement, même si l'ordonnance demeurait secrète. Je pense que le contrôle judiciaire constitue en fait la forme ultime de freins et de contrepoids.

Qu'en pensez-vous, madame Charlet ou madame Patell?

Jeanette Patell: Je vais céder la parole à Mme Charlet pour parler de la nécessité de la surveillance.

Katherine Charlet (directrice principale, Confidentialité, sécurité et sûreté, Affaires gouvernementales et politiques publiques, Google): Merci beaucoup de la question.

Je crois qu'il est instructif d'examiner certains des modèles mis en place. Le contrôle judiciaire est sans aucun doute une protection importante. Il ne s'agit pas de la seule protection. Dans le droit américain, par exemple, un juge fédéral doit effectuer un examen avant d'ordonner une modification technique. Le règlement de l'Union européenne sur les preuves électroniques précise explicitement que toute obligation de déchiffrer des données ou de restructurer des systèmes afin de permettre l'accès ne fait pas partie des pouvoirs prévus par le règlement. La Investigatory Powers Act du Royaume-Uni prévoit un contrôle par un commissaire judiciaire.

Aucune de ces mesures de protection n'est prévue dans le projet de loi C-22. Nous recommandons que le projet de loi prévoie un contrôle judiciaire, mais il ne s'agit peut-être pas de la seule mesure de protection qui pourrait y être ajoutée.

● (1710)

Frank Caputo: Dans la même veine, seriez-vous d'accord…?

Il s'agit ici d'un exercice de comparaison entre les projets de loi et leur rédaction. L'une des lacunes que j'ai constatées dans le cadre du processus du Comité, c'est que nous n'avons pas entendu d'experts en droit européen ni en droit australien, où les métadonnées sont conservées encore plus longtemps, mais je ne sais pas exactement quelles catégories de métadonnées sont conservées. Considérez-vous comme une lacune de cette étude le fait que nous n'ayons pas fait appel à des personnes issues d'autres administrations, comme cela a été soulevé dans le processus du Comité?

En tant qu'observatrice externe, seriez-vous inquiète du fait que le Comité n'examine pas d'autres modèles et n'entende pas des témoins experts en d'autres modèles, pour que nous puissions les comparer afin d'obtenir le meilleur résultat possible?

Katherine Charlet: Je suis d'accord pour dire qu'il serait utile d'examiner ces autres modèles.

D'après notre évaluation, il semble que le projet de loi C-22 serait le seul régime des pays du G7 qui ne prévoit pas de contrôle judiciaire, mais qui prévoit en revanche des pouvoirs d'arrêté ministériel étendus. Il ne fait aucun doute que d'autres personnes pourraient intervenir également sur cette question, mais je pense que c'est une partie intéressante de la discussion.

Frank Caputo: Merci.

Le président: Merci beaucoup de cette réponse.

Je passe maintenant à M. Zuberi, pour six minutes, s'il vous plaît.

[*Français*]

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

[*Traduction*]

Monsieur Israel, je voudrais revenir sur la dernière observation de Mme Charlet. Étant donné que vous faites partie de l'Association canadienne des libertés civiles, pouvez-vous formuler un commentaire concernant ce que Mme Charlet vient de dire au sujet de ce que les autres administrations font?

Tamir Israel: Le régime australien ne prévoit pas d'autorisation judiciaire. C'est l'une des critiques les plus virulentes qui aient été formulées à l'encontre du régime, notamment dans le cadre de l'examen indépendant qui a été mené il y a deux ans. C'était la seule lacune importante qui devait être immédiatement comblée, selon l'examen indépendant. Le régime du Royaume-Uni s'appuie sur un contrôle judiciaire effectué par un commissaire.

Dans le droit canadien, le contrôle judiciaire, en tant que mécanisme, diffère d'une autorisation judiciaire, et il est important de garder les différences à l'esprit. Le contrôle judiciaire est une évaluation de la question de savoir si le décideur a rendu une décision raisonnable en s'appuyant sur les informations dont il dispose. En revanche, quand des juges autorisent un mandat de recherche ou un mandat de cette nature, ils sont les seuls à soupeser les différents facteurs à prendre en considération.

Compte tenu de la nature du projet de loi, il est particulièrement problématique de se fier uniquement au contrôle judiciaire, contrairement à un type d'examen indépendant plus approfondi.

Sameer Zuberi: Dans les autres pays du Groupe des cinq, ou dans des pays comparables, y a-t-il une autorisation judiciaire préalable ou seulement un contrôle judiciaire?

Tamir Israel: Au Royaume-Uni, on effectue un contrôle judiciaire, même si les mécanismes du contrôle judiciaire peuvent être différents de ceux en place ici, au Canada. Ce régime fait actuellement l'objet d'une contestation constitutionnelle.

Aux États-Unis, l'ensemble du régime est supervisé par un organisme de réglementation indépendant — la commission fédérale des communications —, c'est une approche comparable à l'autorisation judiciaire.

Sameer Zuberi: Merci.

Monsieur Neuenschwander…

Erik Neuenschwander: Vous pouvez m'appeler Erik.

Sameer Zuberi: Erik, concernant ce que nous venons d'entendre, connaissez-vous d'autres administrations, et savez-vous comment elles gèrent ces préoccupations pour trouver un juste équilibre entre le fait d'appréhender des acteurs malveillants en ligne et la protection des libertés civiles? Savez-vous ce que d'autres administrations font?

Erik Neuenschwander: D'un point de vue technique, je m'interroge sur l'étendue de ce que ces ordonnances pourraient exiger.

Sameer Zuberi: En ce qui concerne le projet de loi et les aspects techniques que vous avez dit bien connaître, et qui existent dans d'autres administrations, ces dernières partagent-elles notre préoccupation, dans le sens où nous ne pouvons pas nécessairement appréhender tous les acteurs malveillants que nous devrions appréhender dans des délais raisonnables, et que le projet de loi cherche à dissiper et régler cette préoccupation concernant le délai raisonnable?

● (1715)

Erik Neuenschwander: Il est difficile pour moi de parler des autres administrations, mais de manière générale, je dirais que le souhait d'appréhender les acteurs malveillants est universel.

Sameer Zuberi: Je pose la question parce que je m'intéresse à la comparaison.

Madame Charlet, n'hésitez pas à répondre, si vous avez des connaissances sur cette question particulière. Autrement, je vais poursuivre avec d'autres questions.

Katherine Charlet: Google comprend les défis auxquels font face les organismes d'application de la loi, et nous sommes ici pour soutenir ces efforts. Cela fait partie de nos efforts visant à formuler des recommandations constructives sur la manière de modifier le projet de loi.

Sameer Zuberi: Monsieur Neuenschwander, vous avez parlé tout à l'heure du chiffrement. Nous avons entendu plusieurs fois, de la part du gouvernement, qu'il ne lui était pas demandé de désactiver le chiffrement.

Comment se fait-il que vous continuiez à vous présenter devant le Comité alors que votre témoignage porte principalement sur le chiffrement et vos inquiétudes quant à sa désactivation? Comment conciliez-vous ces deux aspects?

Erik Neuenschwander: Encore une fois, je ne suis certainement pas un expert du projet de loi, mais, en l'examinant avec l'équipe, je constate que rien dans le projet de loi lui-même ne prévoit ces mesures de protection contre le chiffrement. J'admets que le projet de loi ne précise pas ce que ces ordonnances exigeraient. C'est en quelque sorte laissé à plus tard.

Pour illustrer cela par une analogie du monde réel, je dirais par exemple que nous craignons qu'il y ait une faille. Je dirais que le projet de loi ne crée pas de faille. Il autorise simplement des ordonnances de confidentialité à créer de force une faille. Notre préoccupation est justifiée parce que, au bout du compte, il y aurait quand même une faille.

Sameer Zuberi: Si vos préoccupations, comme le souligne le gouvernement, sont purement théoriques, avez-vous d'autres amendements ou suggestions concernant ce projet de loi que vous souhaiteriez proposer?

Erik Neuenschwander: Les principales suggestions portent sur la protection explicite du chiffrement et le renforcement de la définition de risque systémique, étant donné que le chiffrement est un aspect parmi d'autres qui, selon nous, pourrait nuire à la sécurité de tous, et nous estimons que cela aurait des conséquences contre-productives pour la société.

Nous accueillerions favorablement un contrôle judiciaire supplémentaire. Nous accueillerions favorablement un assouplissement de certaines des mesures de protection de la confidentialité parce que j'aimerais que l'on puisse tenir des discussions comme celles-ci à l'avenir. Nous avons également quelques préoccupations quant à l'étendue des pouvoirs d'inspection prévus dans le projet de loi, et à la possibilité d'installer l'équipement d'une tierce partie dans des réseaux sécurisés.

Sameer Zuberi: Monsieur Israel, j'aimerais vous donner la parole pour les prochaines minutes, si vous voulez ajouter quoi que ce soit.

Tamir Israel: Une définition qui englobe la nécessité d'exclure toute obligation entraînant des vulnérabilités systémiques devrait prendre en considération la multitude de méthodes et de propositions qui ne cessent d'apparaître pour contourner le chiffrement. La plupart d'entre elles ne compromettent pas directement le chiffrement, mais elles tentent d'y accéder indirectement en le contournant ou en le déjouant, et elles ont néanmoins les mêmes répercussions en ce qui concerne les vulnérabilités qu'elles finissent par créer. Le champ d'application de la définition est limité. J'inviterais également le Comité à vraiment envisager de mettre fin à cela.

Sameer Zuberi: Merci.

[*Français*]

Le président: Merci, monsieur Zuberi.

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Je remercie les témoins d'être des nôtres.

Madame Patell, je vous remercie et vous félicite d'avoir pris la peine de prononcer une partie de votre allocution en français. Votre français est excellent, ainsi que votre prononciation. Alors, merci beaucoup.

Votre entreprise exerce ses activités dans tous les pays membres du Groupe des cinq, si je ne me trompe pas. Donc, vous êtes déjà assujettie à des régimes ou à des lois d'accès légal, comme celles des États-Unis. Si on le compare aux États-Unis, on voit que le Canada a plus de lois, de mécanismes et d'institutions qui protègent la vie privée. Du moins, c'est la lecture que j'en fais.

Alors, étant donné que votre entreprise exerce aussi ses activités aux États-Unis et que vous dites trouver le projet de loi du gouvernement du Canada trop restrictif, pouvez-vous dire comment, selon vous, il se compare à celui des États-Unis?

Jeanette Patell: Je vous remercie de votre question et de votre gentillesse en ce qui concerne mon français.

Je vais céder la parole à ma collègue Mme Charlet, parce qu'il est évident qu'il y a une tension par rapport à la Loi sur la protection des renseignements personnels et au projet de loi C-22.

● (1720)

[*Traduction*]

Je vais céder la parole à ma collègue, Mme Charlet, qui va parler davantage des considérations liées à la protection de la vie privée prévues dans ce projet de loi en particulier, comparativement au régime américain.

Katherine Charlet: Merci beaucoup.

Je pense que la principale comparaison à ce chapitre tient aux principes de protection de la vie privée. Nous pensons que les principes de la protection de la vie privée liés à la minimisation des données et aux contrôles offerts aux utilisateurs, ainsi que le potentiel du projet de loi C-22, pourraient compromettre ces principes.

À titre d'exemple, si l'on regarde la disposition de Google concernant les contrôles offerts aux utilisateurs, nous offrons aux utilisateurs la possibilité de choisir de supprimer leurs données après trois mois. Les exigences relatives à la conservation ou les modifications des produits qui nécessitent que nous apportions des modifications qui exigeraient de conserver les données plus que trois mois iraient à l'encontre des souhaits des utilisateurs. Nous considérons cela avec inquiétude au regard des principes de protection de la vie privée, qui revêtent un caractère universel.

Pour répondre à votre question concernant le droit américain, nous regardons en particulier la loi américaine CALEA. La CALEA interdit explicitement aux gouvernements d'obliger une entreprise à casser le chiffrement. C'est une mesure de protection similaire à celle que le projet de loi C-22 chercherait à mettre en place.

[*Français*]

Claude DeBellefeuille: Des experts et des organismes de la société civile disent que la CLOUD Act des États-Unis confère aux autorités américaines le pouvoir d'exiger l'accès à des données détenues par des entreprises assujetties au droit américain, indépendamment du lieu de stockage des données.

Advenant l'adoption du projet de loi C-22, croyez-vous que le Canada sera équipé pour faire face à cette exigence? Beaucoup d'entreprises et de citoyens ont peur. Ils craignent que, après l'adoption du projet de loi C-22, nos données deviennent accessibles aux pays qui n'ont pas les mêmes préoccupations que nous à l'égard de la protection de la vie privée ou même du respect des droits de la personne.

[*Traduction*]

Katherine Charlet: Je dirais que cette loi a des répercussions mondiales. Le projet de loi C-22 pourrait exiger, dans le cadre d'arrêtés ministériels, qu'une entreprise apporte des modifications au produit. Les possibilités en matière de modification de ces produits sont illimitées, tout comme les exigences de confidentialité qui s'y rapportent. Google et d'autres entreprises sont des entreprises mondiales, et les Canadiens interagissent avec des personnes du monde entier, de sorte qu'une proposition comme celle-ci a des répercussions à l'échelle mondiale.

[*Français*]

Claude DeBellefeuille: Madame Charlet, vous dites que le projet de loi C-22 est plus intrusif sur le plan de l'accès légal que les lois aux États-Unis.

[*Traduction*]

Katherine Charlet: Oui, madame.

La nature pratiquement illimitée des pouvoirs d'obliger les entreprises à modifier leur produit en toute confidentialité et sans contrôle judiciaire, dans le cas des arrêtés ministériels, dépasse tout ce que j'ai pu connaître jusqu'à présent.

[*Français*]

Claude DeBellefeuille: Avez-vous été consultés en amont de la rédaction du projet de loi C-22?

Avez-vous déjà fait part de vos réserves au gouvernement pendant le processus de rédaction du projet de loi?

[*Traduction*]

Katherine Charlet: Nous avons fourni un mémoire contenant des recommandations spécifiques, mais je vais laisser ma collègue, Mme Patell, répondre à votre question plus générale.

Jeanette Patell: Nous avons fait part de ces préoccupations au gouvernement. Je ne crois pas que nous ayons fait partie d'un processus de consultation avant le dépôt du projet de loi, mais nous accueillons favorablement la possibilité de discuter avec le Comité pour trouver des solutions pratiques afin d'aider les organismes d'application de la loi à répondre à leur besoin légitime de mener des enquêtes, tout en assurant la protection de la vie privée des utilisateurs et en garantissant la sécurité de nos produits et de nos services.

Merci de la discussion constructive.

Le président: Merci, madame DeBellefeuille.

Nous allons maintenant passer à Mme Kirkland, pour six minutes, s'il vous plaît.

● (1725)

Rhonda Kirkland (Oshawa, PCC): Merci, monsieur le président.

J'aimerais commencer par simplement…

Le président: J'ai dit six, mais en réalité, c'est cinq minutes.

Rhonda Kirkland: Vous avez dit six, c'est trop tard. Je veux toutefois récupérer ces secondes.

J'aimerais commencer par dire que cela a été fait à la hâte. Nous l'avons dit plus tôt. J'estime que c'est précipité, pour moi, en tant que parlementaire. Pendant la dernière heure, je voulais aborder certaines questions, et je n'ai pas pu le faire, compte tenu de la rapidité avec laquelle tout cela se déroule. Plus tôt, j'ai dit que selon moi, nous devrions veiller à ne pas nous précipiter pour obtenir la sanction royale. Si nous devons nous lancer dans cette voie, il faut que ce soit bien fait.

Je sais que nous n'avons pas reçu certains mémoires au Comité, et je n'en veux à personne pour cela. Je sais qu'il n'y avait aucune mauvaise intention. Je ne reproche pas cela au greffier. Il fallait s'attendre à ce que ce genre de choses se produisent dans un contexte où tout va très vite.

Monsieur Neuenschwander, je crois comprendre que vous avez présenté des mémoires au Comité. Je ne pense pas que le greffier les ait encore transmis, mais heureusement, vous les avez envoyés directement à chacun. Je vous en suis très reconnaissante.

Je voudrais revenir sur une expression que j'entends sans cesse, « porte dérobée ». Je pense que les Canadiens doivent vraiment comprendre ce que cela signifie.

Il y a cinq jours, sur le site Web du gouvernement du Canada, sous la rubrique accès légal, on peut lire « Le projet de loi C 22 n'oblige pas les FSE à créer des « portes dérobées » dans leurs systèmes ni à affaiblir les protections électroniques, y compris le chiffrement ».

Mike McGuire a également dit ceci lors de son témoignage:

> Cette partie ne crée pas de nouveaux pouvoirs pour les forces d'application de la loi ou le SCRS d'intercepter des communications ou d'obtenir des renseignements, pas plus qu'il ne permet l'accès direct du gouvernement aux systèmes des fournisseurs de services électroniques. Il interdit aussi explicitement la création de vulnérabilités systémiques, garantissant ainsi qu'un règlement ou un arrêté ministériel ne fragilise pas le chiffrement et ne crée pas de portes dérobées.

Le ministre a déclaré ceci:

> Cette partie inclut aussi un dispositif de protection explicite pour empêcher l'introduction de vulnérabilités systémiques dans les dispositifs de protection électroniques. Notre gouvernement s'oppose à la création de portes arrière.

Le témoignage d'aujourd'hui semble montrer que ce n'est manifestement pas le cas; j'aurai donc besoin de quelques précisions. Je suis heureuse que vous ayez chacun l'occasion d'apporter cette précision. Je pense qu'il convient de se pencher davantage sur le terme « explicite », parce que cela ne semble pas être explicite dans ce projet de loi. Je sais qu'il y a des moyens pour que cela soit explicite, et je voudrais donc que chacun de vous aborde brièvement ce point. Merci.

Je commencerai par M. Neuenschwander.

Erik Neuenschwander: Je n'ai pas directement entendu ce témoignage, mais à la lecture du projet de loi, nous ne voyons pas certaines de ces affirmations figurer explicitement dans le libellé. On ne mentionne nulle part la protection du chiffrement, et nous serions favorables à l'ajout de cet élément dans le projet de loi. Dans la définition de risque systémique ou de « vulnérabilité systémique », le terme est mentionné, mais sans sa définition.

Les intentions ne transparaissent pas clairement dans le libellé, selon nous. C'est pourquoi, comme vous l'avez dit, nous avons fourni un mémoire écrit et avons proposé des amendements.

Rhonda Kirkland: Merci.

Vous avez utilisé un mot important, qui est « intention ». On nous dit souvent que ce projet de loi n'a pas l'intention de faire X, Y ou Z. Je dirai, encore une fois, que les Canadiens ne se soucient pas vraiment de ce que le projet de loi vise à faire. Ils s'inquiètent de ce à quoi le projet de loi permettra au gouvernement d'avoir accès, et il s'agit d'une véritable inquiétude. Merci d'avoir soulevé ce point.

Je vais d'abord passer à M. Israel, et nous poursuivrons ensuite avec les représentantes de Google.

Tamir Israel: Je partage vos préoccupations quant à l'intention par rapport à l'application. Il a fallu sept ou huit ans avant que la version britannique de ce projet de loi ne soit appliquée pour priver tous les utilisateurs britanniques d'une mesure de sécurité essentielle en matière de chiffrement pour leur sauvegarde sur Apple iCloud. Ce n'est pas l'intention immédiate du gouvernement qui est pertinente. C'est la façon dont le projet de loi pourrait être appliqué au fil du temps.

Dans ce cas, le projet de loi interdit d'imposer des vulnérabilités systémiques, mais cela, par définition, permet la création de vulnérabilités non systémiques, d'une part. Cela laisse de nombreux termes liés à l'électronique dans la définition ouverts à l'interprétation par voie réglementaire, d'autre part.

Un des principaux problèmes avec la tentative permanente de maintenir un chiffrement de bout en bout sécurisé, ce sont les multiples moyens que les gouvernements et les acteurs malveillants ne cessent d'inventer pour contourner le chiffrement. Certains de ces mécanismes compromettent directement le chiffrement. J'ai vu des définitions officielles de « portes dérobées » se limiter à ces exemples, mais d'autres outils qui sont couramment utilisés, comme par exemple, l'analyse côté client, qui, essentiellement, permet d'installer sur l'appareil de chaque utilisateur un outil d'IA chargé de surveiller son contenu avant qu'il ne soit chiffré et transmis, et qui a été jugé par les plus grands technologues en sécurité du monde entier comme créant des vulnérabilités systémiques, ne compromettent pas le chiffrement de la manière que cette exception permettrait d'empêcher. Il faut une exception exhaustive qui exclut toute porte dérobée et tout moyen de contourner le chiffrement.

Merci. Je m'excuse de la longue réponse.

● (1730)

Le président: Merci, madame Kirkland.

C'est au tour de M. Housefather pour cinq minutes, s'il vous plaît.

Anthony Housefather (Mont-Royal, Lib.): Merci beaucoup.

Monsieur Neuenschwander d'Apple, et madame Patell de Google, je vous remercie de votre témoignage et de votre présence ici. J'ai lu vos mémoires. En tant qu'avocat général d'une entreprise informatique, avant de me lancer dans la politique, je suis favorable au renforcement de la protection du chiffrement et à la précision de la définition de « vulnérabilité systémique » et à certaines des autres dispositions que vous avez mentionnées.

J'aimerais réagir à un point que Mme Kirkland a soulevé. Les dispositions habilitantes sont courantes dans tous les cadres de conformité. Elles figurent dans de nombreuses lois fédérales, et elles ne portent pas vraiment spécifiquement sur des dispositions fondamentales en matière d'accès légal de ce projet de loi. Je voulais simplement souligner ce point.

Monsieur Neuenschwander, j'ai lu ce que vous avez dit. Apple a-t-elle déjà comparu devant un comité parlementaire ou présenté un mémoire à un parlement national sur le régime d'accès légal qu'Apple soutient actuellement?

Erik Neuenschwander: Je suis davantage du côté de l'ingénierie que du côté des affaires gouvernementales. Je n'ai pas connaissance de tous les mémoires que nous avons présentés, mais nous soutenons certaines parties du projet de loi C-22 et la modernisation globale afin de permettre aux organismes d'application de la loi de s'améliorer et de devenir plus efficients…

Anthony Housefather: Je comprends cela. Je comprends qu'Apple et Google sont essentiellement favorables à cette idée, mais qu'ils s'opposent à certaines dispositions spécifiques du projet de loi. Je voulais simplement savoir si vous aviez déjà vu un projet de loi dont certaines parties ne vous posaient pas de problème.

Je pense que les gens exagèrent certaines des objections. Je suis d'accord avec certaines des objections que vous avez soulevées, mais je ne pense pas que certaines des affirmations qui ont été faites — par exemple, l'équipement de surveillance qui pourrait être installé dans des appareils et qui oblige les entreprises, même dans le cadre d'arrêts, à installer des équipements de surveillance — sont raisonnables ou logiques. Je ne pense pas qu'elles ressortent clairement dans le libellé du projet de loi.

Voici ma question: avez-vous déjà comparu devant un comité ou présenté un mémoire au Royaume-Uni, en Australie ou aux États-Unis et avez dit « Génial! Nous pensons que ce projet de loi est excellent »?

Erik Neuenschwander: Comme nous le faisons ici aujourd'hui, nous avons souvent participé à des discussions constructives…

Anthony Housefather: Oui, vous êtes allé discuter et contester certaines dispositions dans le projet de loi, ce qui est votre travail.

Nous, en tant que législateurs, devons examiner le projet de loi sous différents angles. Vous avez une obligation spécifique liée à l'entreprise. L'obligation de l'entreprise est de souvent respecter les contrats d'utilisation qu'elle conclut avec les utilisateurs finaux, et de faire ce qui est le mieux dans l'intérêt de l'entreprise, et non pas nécessairement dans l'intérêt national.

J'aimerais savoir si vous avez déjà comparu devant un comité et dit: « Ce projet de loi est excellent. » Je doute que vous l'ayez fait.

Erik Neuenschwander: Respectueusement, je pense que nous nous efforçons ici d'agir dans l'intérêt des utilisateurs, tant au Canada que dans le monde entier, et de veiller à ce que nous puissions fournir les protections les plus solides possibles tout en soutenant l'application de la loi.

Anthony Housefather: Je suis assez d'accord avec vous. Je pense que cela fait partie de l'objectif général.

Permettez-moi également de demander… Vous êtes le directeur principal de la confidentialité. Vous êtes responsable de la confidentialité à Apple.

Erik Neuenschwander: D'un point de vue technologique, oui.

Anthony Housefather: C'est d'un point de vue technologique. C'est exact.

Vous pourriez penser qu'il s'agit d'une question négative, mais elle ne l'est pas. Je pense qu'il s'agit en réalité d'une leçon.

Apple a-t-elle déjà créé un produit que vous avez plus tard regretté? En ce qui concerne la protection de la vie privée, je vais vous donner l'exemple de l'IDFA.

Erik Neuenschwander: Je ne sais pas si j'irais jusque-là.

Pour les personnes qui sont moins férues de technologie, l'IDFA est un identifiant publicitaire. Je pense que c'était tout à fait adapté à l'époque. Ce que nous faisons, c'est que nous continuons de faire évoluer les protections de la confidentialité et du côté de la sécurité, à mesure que le monde évolue.

Anthony Housefather: Vous avez créé quelque chose qui a fini par avoir des répercussions dont vous et votre équipe n'aviez probablement pas conscience lorsque vous l'avez créé la première fois. Les développeurs l'ont en fait utilisé pour aller à l'encontre de ce que vous pensiez être les préférences des utilisateurs. Je m'en souviens.

Erik Neuenschwander: Je pars du principe que les attaques et l'exploitation des données ne cessent de se multiplier et de s'intensifier avec le temps, c'est pourquoi nous continuons d'aller de l'avant et d'innover du côté de la protection. Je ne mettrais pas l'IDFA dans la catégorie des attaques, mais quand on pense aux attaques, de manière générale, nous devons en permanence aller de l'avant pour continuer de protéger les utilisateurs contre les attaques plus importantes.

Anthony Housefather: Je suis d'accord, et c'est pourquoi, quand nous examinons ce projet de loi, nous devons examiner certaines des préoccupations qui ont été exprimées, même si nous ne pensons pas nécessairement qu'elles se concrétiseraient. Nous savons que nous devons penser aux imprévus. Nous devons nous assurer d'éviter de nous retrouver dans une situation qui pourrait avoir des conséquences désastreuses. Je suis en fait favorable à ce que vous dites, parce que, que ce soit ou non dans le projet de loi, je pense que nous voulons répondre aux préoccupations qui ont été exprimées.

Madame Patell, j'ai lu attentivement votre mémoire également. Si nous pouvions limiter la définition de « vulnérabilité systémique », et que nous pouvions garantir ou préciser clairement que le chiffrement ne devait pas être cassé, s'agirait-il des deux principaux points que vous soulèveriez concernant le projet de loi qui permettraient de dissiper les préoccupations que Google a exprimées?

● (1735)

Jeanette Patell: Nous accueillons assurément favorablement toutes les déclarations qui ont été faites en ce qui concerne l'intention du gouvernement, et en particulier le souhait de protéger le chiffrement. Nous voulons simplement voir cela dans le texte du projet de loi lui-même.

Je voudrais mentionner quelques autres points sur lesquels nous avons proposé quatre amendements. Quelques autres concernent à la fois les dispositions relatives à la conservation des métadonnées et le caractère étendu des arrêtés ministériels. C'est quelque chose qui, selon nous, est sans précédent et inutile; nous recommanderions, par conséquent, la suppression des arrêtés ministériels confidentiels également.

Je ne sais pas si ma collègue, Mme Charlet, veut intervenir également ou ajouter quelque chose.

Anthony Housefather: Je pense que le président ne le lui permettrait peut-être pas, parce qu'il semble que mon temps est écoulé.

Le président: Je m'excuse. Malheureusement, votre temps est écoulé, monsieur Housefather, ainsi que le temps pour répondre à ces excellentes questions.

[*Français*]

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

Claude DeBellefeuille: Merci, monsieur le président.

Monsieur Israel, avez-vous les mêmes craintes? Selon vous, le projet de loi accroît-il les risques liés à l'échange d'informations avec des États qui ont un bilan préoccupant en matière de droits de la personne?

[*Traduction*]

Tamir Israel: Oui, à deux égards. D'abord, le projet de loi ouvre la voie à l'adoption d'accords internationaux d'échange d'informations, y compris avec des pays qui ont des antécédents problématiques au chapitre des droits de la personne. C'est un problème.

Un problème connexe est que le régime de conservation des métadonnées n'a pas de limite quant à qui peut avoir accès à ces métadonnées. Une fois qu'elles sont conservées, tout gouvernement peut obliger une entreprise multinationale implantée sur son territoire à divulguer ces données — qui n'auraient pas été conservées si l'entreprise n'était pas obligée de le faire — concernant des personnes au Canada.

[*Français*]

Claude DeBellefeuille: À ce titre, avez-vous déjà fait part de vos craintes aux membres du gouvernement concernant l'échange de renseignements personnels avec des États qui ont un bilan assez préoccupant sur le plan des droits de la personne? Ce n'est pas la première fois que vous faites part de telles craintes aux membres du gouvernement.

[*Traduction*]

Tamir Israel: Nous avons exprimé des préoccupations quant aux accords d'échange de renseignements que j'ai mentionnés. Cependant, nous n'avons pas été informés de l'inclusion du régime obligatoire de conservation des données, avant que le projet de loi C-22 n'ait été déposé; nous n'avons donc pas eu l'occasion de le mentionner à l'avance.

[*Français*]

Claude DeBellefeuille: Selon vous, devons-nous donner plus de pouvoirs à des organismes de reddition de comptes et de surveillance pour surveiller les activités du gouvernement et mieux protéger la vie privée des usagers?

[*Traduction*]

Tamir Israel: Tout à fait. Je pense que l'autorisation judiciaire serait un ajout essentiel ici. Je pense qu'il serait utile d'avoir davantage de surveillance de la part d'organismes comme l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, et le Commissariat à la protection de la vie privée du Canada. C'est un ensemble d'outils très puissants qui sont mis en place.

De plus, en tant qu'organisme de défense des libertés civiles, nous ne comparaissons pas devant de nombreux comités législatifs pour encourager l'élargissement des pouvoirs de la police. Cependant, je tiens à préciser que nous faisons très attention aux occasions où nous intervenons et à la fermeté avec laquelle nous exprimons notre opposition. Ce régime est vraiment large dans sa portée, et c'est précisément pour cette raison que nous sommes ici pour faire part de nos préoccupations.

[*Français*]

Le président: Merci, madame DeBellefeuille.

Monsieur Baber, vous avez la parole pour cinq minutes.

[*Traduction*]

Roman Baber (York-Centre, PCC): Merci.

Monsieur Neuenschwander d'Apple Inc., bienvenue au Comité de la sécurité publique et nationale.

Je lis un commentaire que l'entreprise Apple a fait, dans le *Globe and Mail*, selon lequel ce projet de loi pourrait permettre au gouvernement canadien, je traduis, « d'obliger les entreprises à casser le chiffrement en installant des portes dérobées dans leurs produits — une chose qu'Apple ne fera jamais ».

Aux fins du compte rendu, les conservateurs s'opposent au contournement du chiffrement. Cependant, j'aimerais que vous donniez suite à ce commentaire formulé par Apple, selon lequel le contournement du chiffrement en installant des portes dérobées dans vos produits est une chose que vous ne ferez jamais. Disons que ce projet de loi est adopté, dans sa forme actuelle, et que les libéraux parviennent à leurs fins. Que se passe-t-il ensuite?

● (1740)

Erik Neuenschwander: Nous resterons déterminés à offrir aux Canadiens le plus haut niveau de sécurité possible. Nous espérons que le projet de loi sera modifié pour prévoir ces mesures de protection explicites relatives au chiffrement afin d'éviter de créer des tensions entre ces aspects.

Roman Baber: Je comprends cela, mais qu'en est-il si les conservateurs échouent, et que vous soyez obligés d'installer une porte dérobée et de casser le chiffrement? Que fera alors Apple? Serait-ce une première fois pour Apple, ou cela signifiera-t-il qu'Apple quittera le Canada?

Erik Neuenschwander: Je ne peux pas spéculer sur ce qui se passerait dans cette situation. Grâce à cette discussion et à ce dialogue continu, nous espérons, encore une fois, que des modifications positives seront apportées au projet de loi.

Roman Baber: Pouvez-vous nous dire ce qui s'est passé au Royaume-Uni concernant la même question, quand Apple a décidé que le projet de loi, dans sa forme actuelle, était inadmissible pour lui?

Erik Neuenschwander: Apple a déposé des observations à la fois lors du débat initial sur le projet de loi, puis des observations publiques pendant la phase d'amendement, plus récemment.

Roman Baber: D'accord.

Je m'adresse aux représentantes de Google; je vois dans votre mémoire une observation selon laquelle « Google n'a jamais conçu de porte dérobée ni tout autre mécanisme visant à contourner le chiffrement de bout en bout de ses produits ». Cela se limite-t-il au Canada, ou cela s'applique-t-il à l'échelle mondiale?

Jeanette Patell: C'est à l'échelle mondiale.

Roman Baber: Autrement dit, ce serait une première. Si ce projet de loi va de l'avant et qu'il est adopté, dans sa forme actuelle, Google serait forcé de faire quelque chose qu'il n'a jamais fait ailleurs dans le monde.

Jeanette Patell: Si ce projet de loi est adopté, dans sa forme actuelle, le ministre aurait le pouvoir d'exiger de Google ou d'autres fournisseurs de services électroniques, qu'ils se conforment aux obligations fondamentales prévues au paragraphe 5(2) proposé.

Nous sommes ici aujourd'hui pour veiller à ce que le Comité prenne le temps de discuter et de parvenir à un projet de loi qui soit applicable et qui trouve le juste équilibre entre la préservation de la sécurité des utilisateurs et le soutien des efforts des forces de l'ordre.

Roman Baber: Merci.

Vous avez écrit que la portée de ces éventuelles obligations est pratiquement « illimitée ». Pourriez-vous nous parler de certaines des limites qui pourraient être testées par ce projet de loi et qui n'ont pas été auparavant testées, à part le contournement du chiffrement?

Jeanette Patell: En fait, ce qui est en jeu ici, ce sont des niveaux complexes d'architecture de sécurité qui vont bien au-delà du simple chiffrement.

Je pense que ma collègue, Mme Charlet, peut parler de ce que cela pourrait englober.

Katherine Charlet: Je dirais que la raison pour laquelle nous considérons ces obligations comme étant pratiquement illimitées, c'est que les pouvoirs des arrêtés obje ainsi que les obligations fondamentales des fournisseurs sont, en réalité, pratiquement illimités en ce qui concerne les notifications pouvant être adressées aux personnes; l'installation, l'utilisation, l'exploitation, la gestion et les essais de tout appareil ou équipement; ainsi que de nombreux autres pouvoirs énumérés qui vont au-delà de certains des pouvoirs accordés dans d'autres pays à travers le monde.

Roman Baber: Si je comprends bien votre observation, non seulement la portée de ces arrêtés ministériels est éventuellement illimitée, mais le cadre de ces derniers leur offre également une immunité contre tout contrôle ou toute obligation de rendre des comptes, car il n'est pas possible de faire appel de ces arrêts.

On ne peut pas aller devant un tribunal et dire que l'on ne se sent pas à l'aise de faire ce que les arrêtés ministériels exigent de faire. Il n'y a aucun contrôle judiciaire. N'est-ce pas?

Katherine Charlet: Oui, tout cela est fait en secret.

Je pense qu'il y a une possibilité d'appel. Cependant, pendant la période d'appel, il n'y a aucun sursis, donc si l'entreprise fait l'objet d'un arrêté, elle serait obligée de mettre en œuvre le changement avant d'obtenir une décision concernant un appel.

Roman Baber: J'aimerais préciser que le ministre de la Sécurité publique, le gouvernement, le SCRS et la GRC peuvent déjà demander et obtenir un mandat de recherche et demander à Google de répondre aux demandes de renseignements. N'est-ce pas?

Katherine Charlet: Oui.

Roman Baber: Je ne comprends pas vraiment pourquoi il faut en faire autant.

J'aimerais prendre un instant pour parler de...

Le président: Malheureusement, le temps est écoulé, monsieur Baber. Je m'en excuse.

Je vais passer à M. Powlowski, pour cinq minutes, s'il vous plaît.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Parce que je suis un boomer, mes enfants m'en remontrent dès qu'il est question d'informatique, et je dois avouer que j'essaie encore de comprendre ce projet de loi.

Le projet de loi porte sur les fournisseurs de services et les fournisseurs de données. Monsieur Neuenschwander, Apple fait-il partie de l'une de ces catégories, ou des deux?

● (1745)

Erik Neuenschwander: Je suppose que c'est le cas, mais cela ne semble pas précisé dans le projet de loi.

Marcus Powlowski: Comment définiriez-vous un fournisseur de services et un fournisseur de données?

Erik Neuenschwander: Je ne me considère pas comme un expert du projet de loi, mais je pense qu'il s'agit plutôt d'examiner les fournisseurs de services qui détiennent des renseignements dans le cadre de leurs activités.

Marcus Powlowski: Je m'excuse. Parlez-vous du fournisseur de services ou du fournisseur de données? Je n'ai peut-être pas à vous demander cela.

Parlez-moi des conséquences financières de ce projet de loi sur Apple. Quelles conséquences financières a-t-il sur vous?

En particulier, il y a une exigence relative à la conservation des métadonnées pour une période allant jusqu'à un an. Vous êtes un informaticien. Vous êtes un ingénieur. Comment conservez-vous les métadonnées? Où sont-elles conservées? Sont-elles dans votre nuage? Où cela a-t-il lieu, et combien la conservation de ce genre de données coûte-t-elle à votre entreprise?

Erik Neuenschwander: Essentiellement, je ne pense pas que nous nous concentrons trop sur les coûts. Nous nous concentrons sur les risques qui pourraient découler de cette conservation accrue des métadonnées.

Actuellement, nous conservons le minimum de données nécessaires à la fourniture du service. D'après ce que je comprends du libellé actuel du projet de loi, c'est qu'il pourrait exiger de conserver davantage de données au-delà de cette période. Ce que nous examinons ici, c'est simplement un volume plus important de données qui pourraient être piratées par un cybercriminel et utilisées pour commettre d'autres crimes.

Nous ne savons pas si cela s'est déjà produit chez Apple jusqu'à présent, et je vais toucher du bois, mais c'est en partie parce que nous réduisons ce profil de menace autant que possible.

Marcus Powlowski: Pensez-vous que les conséquences financières soient un sujet de préoccupation pour votre entreprise?

Erik Neuenschwander: En tant qu'ingénieur, ce n'est probablement pas mon domaine, mais encore une fois, je m'inquièterais surtout pour la sécurité.

Marcus Powlowski: Permettez-moi de poser la même question aux représentantes de Google.

Vous considérez-vous comme un fournisseur de services, un fournisseur de données ou les deux?

Jeanette Patell: Comme Apple, certaines de ces définitions sont laissées à la discrétion d'une réglementation future; nous attendons donc des précisions quant à leur champ d'application. Si nous comprenons bien, dans les deux cas, nous serons concernés par le projet de loi.

Marcus Powlowski: Je suis un peu surpris. Compte tenu de la taille de Google et d'Apple, et de leur importance, je trouve un peu déconcertant que le projet de loi puisse être à ce point vague que vous ne sachiez même pas s'il s'applique à vous.

Jeanette Patell: C'est un excellent point en ce qui concerne l'occasion d'apporter des éclaircissements et des précisions dans le projet de loi pour que les entreprises qui exercent leurs activités au Canada comprennent clairement les obligations qui s'appliquent à elles.

Marcus Powlowski: Puis-je vous poser quelques questions sur les conséquences financières de ce projet de loi? Je devrai peut-être poser la question de manière plus générale avant d'aborder les détails sur la conservation des métadonnées jusqu'à une période d'un an. De manière générale, selon vous, quelles sont les répercussions financières pour Google?

Jeanette Patell: Comme Apple, les considérations financières n'ont pas été notre principale considération. Nous nous concentrons sur les vulnérabilités que ce projet de loi pourrait créer pour notre...

Marcus Powlowski: Permettez-moi de contester cela. Vous êtes des entreprises. Je trouve que vous vous en sortez très bien en tant qu'entreprise. Il se peut même que je détienne des actions de votre entreprise, qui — merci beaucoup — se porte très bien, mais je pense que votre entreprise a pour mission et pour obligation de veiller à ses résultats financiers. Je suis un peu surpris que vous ne soyez pas préoccupés par les répercussions financières de ce projet de loi.

Jeanette Patell: Notre objectif ici est avant tout de protéger les utilisateurs et les systèmes que nous exploitons. Nous consacrons beaucoup de ressources à ce chapitre pour nos utilisateurs du monde entier, notamment grâce à une partie de notre formidable équipe basée à Montréal.

Peut-être que Mme Charlet peut parler de ce que nous constatons en ce qui concerne les contraintes liées à la conformité que pourraient entraîner des régimes de ce type.

Katherine Charlet: Je suis d'accord avec les observations qui ont été formulées jusqu'à présent sur les coûts, mais j'ajouterais que les entreprises internationales cherchent à créer une expérience produit unique, et non pas à devoir mettre en place une centaine d'expériences produits et de systèmes différents à travers le monde.

Bien sûr, nous sommes une grande entreprise. Nous pouvons gérer des régimes de conformité complexes, mais, en ce qui concerne l'expérience produit, il est préférable que les utilisateurs bénéficient d'une expérience similaire lorsqu'ils se déplacent à l'étranger.

Marcus Powlowski: Nous avons déjà entendu dire que...

Le président: Je m'excuse, monsieur Powlowski, de vous interrompre, mais c'est mon devoir, puisque le temps est écoulé pour la deuxième heure.

Merci aux témoins d'avoir pris le temps d'être ici, soit en personne, soit virtuellement.

Nous allons suspendre la séance pour quelques instants le temps que l'autre groupe arrive. Encore une fois, merci, et passez une bonne journée.

● (1750)

(Pause)

● (1755)

[*Français*]

Le président: Nous reprenons la séance. C'est la troisième partie de la réunion. Nous recevons de nouveaux témoins, auxquels nous souhaitons la bienvenue.

Nous recevons, de la Gendarmerie royale du Canada, M. Mathias Van Laer, qui est ici avec nous.

[*Traduction*]

J'invite tout le monde à être un peu plus attentif.

[*Français*]

De l'Association canadienne des chefs de police, nous accueillons M. Thomas Carrique, commissaire.

De la Ville de Brampton, nous accueillons M. Patrick Brown, maire de Brampton.

Je souhaite la bienvenue à nos témoins.

Nous commençons maintenant les présentations de cinq minutes.

Monsieur Van Laer, vous avez la parole.

[*Traduction*]

Mathias Van Laer (sergent d'état-major retraité, réserviste, Gendarmerie royale du Canada): Bonjour, monsieur le président et mesdames et messieurs les membres du Comité. Merci de m'avoir invité à prendre la parole aujourd'hui, alors que nous nous réunissons sur le territoire traditionnel et non cédé de la nation anishinaabe; nous reconnaissons la présence permanente des peuples des Premières Nations, Inuits et Métis dans cette région.

Je m'appelle Mathias Van Laer. J'ai été membre de la GRC pendant 25 ans et j'ai fini par prendre ma retraite en 2022 en tant que sergent d'état-major.

[*Français*]

J'aimerais aussi souligner que je suis d'origine francophone. C'est avec plaisir que je répondrai à vos questions dans la langue officielle de votre choix.

[*Traduction*]

Pendant mon service, j'ai été sous-officier responsable du Groupe intégré de lutte contre l'exploitation des enfants, le GILEE, de la division E de la GRC, situé dans le district du Lower Mainland, mais qui représente l'ensemble de la province de la Colombie-Britannique. Après mon départ à la retraite en 2022, j'ai réintégré la GRC en tant que gendarme de réserve pour la ville de Kamloops, en Colombie-Britannique, pour poursuivre mon travail au sein de leur unité des crimes sexuels, où je participe activement aux enquêtes en cours, je prépare les autorisations judiciaires et supervise la prise en charge de toutes les enquêtes sur l'exploitation sexuelle des enfants en ligne dans la ville de Kamloops, en fournissant des conseils, des orientations et des formations.

Pour vous donner un peu de contexte, les groupes de lutte contre l'exploitation des enfants de la GRC sont composés d'équipes spécialisées chargées de prévenir et de détecter des crimes impliquant l'exploitation sexuelle des enfants, à la fois en ligne et hors ligne, et d'enquêter sur ces crimes. Leur mandat est axé sur la protection des victimes vulnérables, l'identification et l'appréhension des délinquants, et elles travaillent en collaboration avec les partenaires nationaux et internationaux pour perturber les réseaux impliquant du matériel d'abus et d'exploitation pédosexuelle. Les principales priorités comprennent la collecte proactive de renseignements, l'identification et le soutien des victimes, l'analyse judiciaire numérique et les initiatives de sensibilisation du public afin de réduire les risques et d'augmenter les signalements.

Pendant mon service au GILEE de la Colombie-Britannique, je me suis efforcé de répondre à la demande croissante, en matière d'enquêtes sur l'exploitation sexuelle des enfants en ligne, alimentée par l'utilisation croissante d'Internet. En collaboration avec les services d'analyse numérique de la GRC, le GILEE de la Colombie-Britannique soutient les organismes d'application de la loi dans toute la Colombie-Britannique, s'efforce d'identifier et d'aider les enfants victimes, et identifie les délinquants, afin d'étayer des poursuites pénales fondées.

En tant qu'enquêteurs, nous adaptons constamment nos techniques d'enquête pour nous adapter aux criminels, surtout ceux qui sévissent dans l'espace numérique et qui portent le plus grand préjudice aux Canadiens vulnérables, y compris les enfants. Le projet de loi C-22, Loi concernant l'accès légal, moderniserait nos lois, afin que les services de police canadiens puissent enquêter sur les crimes et cibler ceux qui s'attaquent aux personnes vulnérables.

Les groupes de lutte contre l'exploitation des enfants de la GRC s'appuient de plus en plus sur les outils numériques, l'analyse des données et la collaboration avec les partenaires du renseignement pour faire avancer les enquêtes. Les amendements apportés au Code criminel, proposés dans le cadre du projet de loi C-22, permettraient d'améliorer les délais et l'uniformité dans l'obtention des éléments de preuve numériques, en particulier dans les cas urgents ou qui évoluent rapidement.

Les enquêtes sur l'exploitation des enfants dépendent essentiellement de la traçabilité des adresses IP, des renseignements de l'abonné et de la conservation des données volatiles en ligne avant qu'elles ne soient supprimées ou effacées. Des dispositions renforcées en matière d'accès légal pourraient simplifier les ordonnances de communication et les demandes de conservation, et permettraient aux enquêteurs d'agir plus rapidement pour identifier les suspects et protéger les victimes.

La protection des enfants reste une priorité fondamentale de la GRC. Les équipes sont engagées à protéger des victimes vulnérables, à poursuivre les délinquants et à s'adapter aux menaces en ligne en constante évolution, grâce à des partenariats solides et des outils d'enquête modernes. Que ce soit par l'application de la loi, le soutien aux victimes ou les efforts de prévention, la GRC continue de placer la sécurité et le bien-être des enfants au cœur de sa mission, tout en reconnaissant l'importance capitale de les protéger contre les préjudices dans tous les environnements.

Merci beaucoup. Je répondrai volontiers à vos questions.

● (1800)

[*Français*]

Le président: Merci beaucoup, monsieur Van Laer.

Monsieur Carrique, vous avez la parole pour cinq minutes.

[*Traduction*]

Le commissaire Thomas Carrique (président, Association canadienne des chefs de police): Mesdames et messieurs les membres du Comité, merci de me donner la possibilité de prendre la parole concernant le projet de loi C-22.

Aujourd'hui, pratiquement toutes les enquêtes criminelles sérieuses comportent un volet numérique. Les groupes du crime organisé, les prédateurs d'enfants, les fraudeurs, les délinquants violents et les extrémistes comptent tous sur les communications, les plateformes numériques, les outils anonymes et les services de forum de discussion chiffrés pour coordonner leurs activités criminelles, échapper à la détection, faire échouer les poursuites et, au bout du compte, victimiser les Canadiens innocents. Les criminels tirent parti de l'infrastructure numérique et du chiffrement, alors que la police est freinée par un projet de loi obsolète qui ne donne pas la priorité à la sécurité publique.

Le projet de loi C-22 ne porte pas sur l'élargissement des pouvoirs non contrôlés de la police. Il vise à s'assurer que les enquêtes autorisées par la justice puissent fonctionner efficacement dans un environnement numérique complexe et en constante évolution. À l'avantage des acteurs malveillants, les débats sur l'accès légal se concentrent trop souvent exclusivement sur les droits à la protection de la vie privée des suspects et les intérêts financiers des géants de la technologie, tout en négligeant les droits des victimes à la sécurité, à la justice et à une intervention rapide.

La police ne demande pas une surveillance étendue, et le projet de loi C-22 ne l'autorise pas non plus. Il n'autorise pas l'interception de communications sans mandat. Il ne supprime pas le contrôle judiciaire. Il ne fournit pas un accès illimité à l'historique de navigation ou au contenu des médias sociaux. Le projet de loi préserve les mesures de protection prévues dans la Charte et conserve les exigences liées à l'autorisation judiciaire pour faire avancer les techniques d'enquête.

Le projet de loi C-22 porte également sur les mesures d'enquête concrètes. Par exemple, il prévoit une confirmation confidentielle du processus de service, en répondant par un simple oui ou non, pour que les enquêteurs puissent déterminer quel fournisseur de télécommunications détient les registres pertinents avant de passer un temps précieux à demander des autorisations judiciaires pour obtenir des registres qui n'existent peut-être simplement pas. Il prévoit un processus d'ordonnance de communication pour obtenir les renseignements de base des abonnés fondé sur des motifs raisonnables de soupçonner, permettant ainsi aux enquêteurs de faire avancer l'enquête préliminaire. Il porte également sur les délais liés aux éléments de preuve détenus à l'étranger dans les affaires où les enquêteurs doivent actuellement recourir à des procédures d'aide judiciaire qui prennent plusieurs mois, période durant laquelle les preuves disparaissent souvent. En fait, le projet de loi C-22 prévoit des règles législatives claires dans des domaines où les tribunaux, les fournisseurs et les enquêteurs se heurtent actuellement à des interprétations non uniformes et à l'incertitude juridique.

Le projet de loi C-22 empêche les criminels d'être à l'abri, en imposant aux fournisseurs de services électroniques l'obligation de mettre en place et de maintenir des systèmes permettant de fournir à la police les communications et les renseignements qu'elle est légalement autorisée à obtenir, et qui sont nécessaires pour faire avancer les enquêtes criminelles.

Il est important de noter que le projet de loi C-22 n'est pas un outil de surveillance; c'est un cadre d'accès légal. Les métadonnées seraient conservées pour une durée maximale d'un an, y compris les renseignements comme la date, l'heure, la durée et l'origine de la transmission. Il est essentiel de préciser qu'il n'y aura aucune obligation de conserver des contenus tels que des courriels, des historiques de navigation ou des activités sur les médias sociaux.

De plus, la conservation n'est pas synonyme d'accès. L'autorisation judiciaire sera tout de même nécessaire. Les métadonnées constituent le strict minimum d'information susceptible d'aider les enquêteurs dans le cadre d'enquêtes complexes, comme sur les homicides, l'exploitation sexuelle internationale d'enfants, l'extorsion, le vol d'automobiles transfrontalier, la traite de personnes et le trafic de drogues et d'armes à feu. Ces types de crimes peuvent largement dépasser la période d'un an d'enquêtes qui peuvent nécessiter un accès légal.

En l'absence de soupçon raisonnable d'activité criminelle, la police ne demandera pas et n'obtiendra pas légalement, et ne pourrait pas le faire, la communication de métadonnées concernant un citoyen canadien vaquant à ses occupations quotidiennes. De plus, d'autres mesures de protection sont prévues dans le projet de loi. Le règlement conçu par le gouverneur en conseil doit tenir compte des répercussions sur la protection de la vie privée et la cybersécurité, la faisabilité, des coûts pour les fournisseurs et des répercussions sur les consommateurs, et le commissaire au renseignement doit approuver des ordonnances avant qu'elles ne soient délivrées au fournisseur de services électroniques.

Le projet de loi C-22 empêche également toute exigence susceptible d'amener un fournisseur de services électroniques à créer une vulnérabilité systémique, définie dans le projet de loi comme étant « un risque sérieux qu'une personne puisse accéder à de l'information sécurisée sans en avoir le droit ou l'autorisation ».

● (1805)

Pour être franc, d'un point de vue de l'application de la loi, les préoccupations exprimées par certaines grandes entreprises de télécommunications et par les défenseurs de la vie privée concernant le chiffrement et la cybersécurité sont exagérées. Le projet de loi, dans sa forme actuelle, n'oblige pas les entreprises à affaiblir le chiffrement ou à créer des vulnérabilités; selon le cadre législatif, il permet plutôt de s'assurer que les fournisseurs de services électroniques ne servent pas de refuge aux activités criminelles et terroristes et ne compromettent pas la sécurité publique à l'échelle locale, nationale et internationale.

Le président: Je m'excuse de vous interrompre, monsieur le commissaire, mais pourriez-vous conclure en cinq ou dix secondes?

le comm. Thomas Carrique: Oui, monsieur.

Pour conclure, je serai heureux de répondre à vos questions.

Merci.

Le président: Merci. Je vous en suis très reconnaissant.

Je vais maintenant me tourner vers M. Brown.

M. Brown a beaucoup de mérite d'être ici aujourd'hui, puisqu'aujourd'hui, c'est son anniversaire. Nous n'allons pas prendre le temps de vous chanter un joyeux anniversaire, car nous ne voulons pas empiéter sur le temps qui vous est alloué.

Joyeux anniversaire, monsieur le maire, et vous aurez, vous aussi, cinq minutes.

Patrick Brown (maire, Ville de Brampton): J'allais fêter mon anniversaire, mais quand j'ai appris que vous parliez d'un sujet aussi important, je ne voulais pas manquer l'occasion de prendre la parole au nom des résidents de Brampton et de la région de Peel, où nous avons, malheureusement, fait face à une importante activité criminelle, où le projet de loi C-22 aurait pu faire un monde de différence.

Je voudrais faire part de quelques points au Comité, aujourd'hui.

Le crime organisé est très complexe. Je porte deux casquettes, celle de maire de Brampton, et celle de membre de la Commission des services policiers de Peel. Les observations fort éloquentes du commissaire Carrique sont les mêmes que celles que j'entends de la part des hauts gradés de la police. Cela pourrait être l'outil d'enquête le plus important pour la police depuis que les preuves par l'ADN ont changé les règles du jeu.

Le crime organisé ne veut pas que le Canada mette à jour son projet de loi sur l'accès légal. Pour être franc, il peut mener des activités criminelles en toute impunité dans le pays. La police a les mains liées, et c'est regrettable. Il y a davantage de victimes et davantage de crimes évitables. Je suis certain que si le Comité ou le Parlement du Canada hésite sur ce projet de loi ou le reporte, le gang Bishnoi, le cartel de Sinaloa et les For Brothers seront ravis, mais il y aura davantage de victimes.

Je viens d'une collectivité où j'ai vu de trop nombreux cas d'exploitation d'enfants, de traite de personnes et d'extorsion. Et il ne faut pas me lancer sur les extorsions, parce qu'elles ont terrorisé notre collectivité. Je peux vous dire que, l'année dernière, dans la région de Peel, nous avons eu 476 cas d'extorsion touchant des familles et des entreprises. Ce projet de loi est absolument essentiel pour nous afin que nous puissions tenir ces organisations criminelles responsables.

Dans le cas des extorsions, les ordonnances de communication peuvent prendre trois, quatre ou cinq semaines, et parfois même plus. Il y a constamment des retards. En raison des retards relatifs aux ordonnances de communication, les enquêtes stagnent.

Les enquêtes policières sont extrêmement efficientes quand la police dispose des outils nécessaires pour faire son travail, et je peux vous dire que le crime organisé utilise tous ces outils technologiques modernes. Quand les enquêteurs doivent attendre 45 jours pour obtenir des informations cruciales, les vidéos des caméras locales disparaissent, les éléments de preuve essentiels disparaissent, et davantage de victimes innocentes sont traumatisées.

Certaines victimes m'avaient appelé. Un père m'avait appelé et m'a dit « mes enfants n'arrivent pas à dormir depuis que notre maison a été la cible de coups de feu ». Pouvez-vous imaginer que vos enfants n'arrivent pas à dormir pendant des mois parce qu'ils ont été terrorisés par une extorsion? On aurait pu empêcher ces extorsions, si la police disposait des outils nécessaires pour faire son travail.

Je sais que l'opposition a exprimé des préoccupations quant à la version initiale de ce projet de loi. Cependant, je tiens à vous dire — et je sais que la police de Peel a apporté sa contribution — qu'il s'agit d'une approche équilibrée qui offre à la police les mêmes outils que ceux dont disposent les autres pays du Groupe des cinq. Je sais que des lobbyistes représentant des sociétés de technologie feront activement pression contre ce projet de loi pour leurs propres raisons, mais si cela fonctionne dans les pays du Groupe des cinq, où il existe un équilibre entre la protection de la vie privée et la mise à la disposition de la police des outils nécessaires pour lui permettre d'accomplir son travail, nous pouvons trouver cet équilibre au Canada.

J'ai participé au caucus des maires des grandes villes, où nous avons fait du lobbying auprès du premier ministre Carney, précisément pour fournir aux forces policières locales cet outil qui est si indispensable. Pour ceux qui ont des préoccupations liées à la protection de la vie privée, mon message est le suivant: ne commettez pas de crime. Ne soyez pas impliqué dans un crime haineux. Ainsi, on ne portera pas atteinte à votre vie privée.

On entend les forces de l'ordre dire qu'il sera seulement utilisé lorsqu'il y a un motif raisonnable de soupçonner un crime. Si l'on a une preuve vidéo de quelqu'un impliqué dans un crime, il ne faudrait pas attendre 45 jours pour obtenir cette information numérique.

C'est la nouvelle guerre. Je lis les rapports de police et je les étudie. Je peux vous dire que j'ai sans cesse demandé à la haute direction de la police régionale de Peel combien de temps une enquête prendrait, si nous avions l'accès légal. À maintes reprises, on m'a répondu qu'une enquête prendrait bien moins de temps. Dans le cas des enquêtes qui sont au point mort, cela aurait pu faire la différence en permettant de prévenir les crimes et d'éviter de nouvelles victimes; c'est pourquoi j'exhorte le Comité à ne pas tergiverser ni reporter ce projet de loi.

S'il y a des rajustements et des amendements raisonnables à faire, il y a ici des parlementaires raisonnables. Parvenez, s'il vous plaît, à un consensus, mais ne tergiversez pas et ne reportez pas le projet de loi. Les seules personnes que vous satisferez en tergiversant ou en tardant à communiquer ces informations cruciales que les forces de l'ordre demandent avec insistance, ce sont les membres du crime organisé.

Je suis heureux de prendre la parole devant cet honorable comité, aujourd'hui.

● (1810)

Le président: Merci, monsieur Brown.

Nous allons maintenant passer à M. Caputo; allez-y, s'il vous plaît, vous avez six minutes.

Frank Caputo: Merci.

Joyeux anniversaire, monsieur le maire. C'est un plaisir de faire votre connaissance sur Zoom.

Monsieur le commissaire Carrique, je suis ravi de vous voir de nouveau; j'ai eu le plaisir de vous rencontrer maintes fois.

Bonjour, Monsieur Van Laer, heureux de vous voir.

M. Van Laer et moi-même avons travaillé ensemble sur des enquêtes concernant le matériel de maltraitance et l'exploitation sexuelle d'enfants. L'une des raisons pour lesquelles je l'ai invité ici, et que je tenais à l'entendre, c'est que personne ne nous a encore dit ce que cela fait de défoncer une porte ou encore quel type de métadonnées on cherche quand on enquête sur des cas d'exploitation sexuelle d'enfants.

Monsieur Van Laer, mes questions s'adresseront à vous, pour le moment.

Le projet de loi porte sur les métadonnées. Connaissez-vous bien les métadonnées dans le contexte des cas de matériel d'exploitation sexuelle d'enfants et de leurre au moyen d'Internet? Je présume que vous connaissez les métadonnées et que vous savez comment tout cela fonctionne.

Mathias Van Laer: Oui.

Frank Caputo: C'est quelque chose dont vous avez l'habitude, sur le terrain. N'est-ce pas?

Mathias Van Laer: En effet. Il y a, bien sûr, des couches de métadonnées.

Frank Caputo: Oui.

Vous êtes intervenu dans des cas dont nous n'avons peut-être jamais entendu parler, jusqu'au cas d'Amanda Todd, en Colombie-Britannique.

Mathias Van Laer: C'est exact.

Frank Caputo: Les métadonnées sont-elles utiles dans les enquêtes sur les cas d'exploitation sexuelle d'enfants? Pourriez-vous l'expliquer au Comité? C'est la première fois que nous en entendons parler.

Mathias Van Laer: Tout à fait.

Tout d'abord, le terme métadonnées couvre un champ très large, il pourrait donc être utile de nous assurer de bien comprendre ce que nous entendons par « métadonnées ». C'est l'information recueillie par un fournisseur des services électronique, et chaque élément peut être considéré comme une métadonnée.

Au bout du compte, la police n'identifie pas seulement l'abonné à Internet. L'abonné à Internet est simplement la personne qui paie la connexion Internet. Notre travail, pour satisfaire la poursuite, consiste à identifier qui se cache derrière le clavier. Pour ce faire, nous devons examiner en profondeur les activités sur Internet, afin d'identifier l'utilisateur soupçonné plutôt que le simple abonné. L'abonné est une pièce du casse-tête, qui mènera, nous l'espérons, à l'utilisateur. Nous ne pouvons pas identifier un utilisateur si nous ne pouvons pas voir ses traces; nous pourrions l'identifier à partir de certaines de ses traces sur Internet, si vous comprenez ce que je veux dire.

Frank Caputo: Disons qu'on vous transmet l'adresse IP d'une personne soupçonnée d'exploitation sexuelle d'enfants. Que faites-vous?

Mathias Van Laer: Présentement, nous sommes tenus de rédiger une ordonnance de communication pour obtenir le nom et l'adresse de l'abonné. Ce processus exige beaucoup d'heures-personnes. La rédaction de l'ordonnance de communication est longue, mais il revient au fournisseur de services Internet de nous fournir le résultat de cette ordonnance. Cela peut prendre jusqu'à 30 jours, parfois plus.

Évidemment, nous ne nous arrêtons pas là. Une fois que l'adresse IP est liée à un abonné, nous avons une adresse. Une fois que nous avons l'adresse, nous commençons notre enquête sur cette adresse et ses résidents. Puis, la plupart du temps, cela mène à un mandat de perquisition. Nous devons convaincre les tribunaux et fournir des motifs raisonnables et plausibles pour lesquels nous croyons qu'une infraction a été commise à ce domicile et qu'il s'y trouve des preuves. Ensuite, nous passons la porte du domicile pour saisir les ordinateurs et les appareils électroniques et nous cherchons les traces qui nous ont menés jusqu'à cette porte.

Gardez à l'esprit que l'adresse IP ne tombe pas du ciel. Elle a déjà été signalée à notre attention. Elle nous a été transmise par un fournisseur de services électroniques qui signale de lui-même des activités criminelles en ligne. Le fournisseur estime qu'il s'agit d'activités criminelles et c'est pourquoi il les signale; alors, le dossier arrive sur notre bureau, sans que nous en fassions la demande. Nous recevons des rapports soumis volontairement par les fournisseurs de services électroniques.

● (1815)

Frank Caputo: Une fois que vous avez cette information — vous avez défoncé la porte, pour ainsi dire, et saisi plusieurs appareils —, quel est l'échéancier de l'enquête? Quel rôle pourraient jouer les métadonnées dans l'identification et l'arrestation d'un prédateur d'enfants?

Mathias Van Laer: C'est là qu'intervient l'analyse médico-légale numérique. Des experts en la matière examineront les ordinateurs. Ils pourront voir tout ce qui s'est fait sur l'ordinateur à une date et une heure données. Nous essayons de faire correspondre l'activité de l'ordinateur avec celle du délinquant, et c'est ainsi que nous découvrons qui se cache derrière le clavier.

Le fournisseur de services électroniques recueille le nom d'utilisateur, l'adresse IP et des informations liées au profil. Parfois, dans les cas complexes, c'est ce qui nous permet de déterminer qu'un même utilisateur utilise plusieurs profils, parce que c'est possible. Mes collègues, qui comparaissent aussi aujourd'hui en tant que témoins, parlent des enquêtes complexes. La plupart du temps, nous avons affaire à un seul délinquant, à une personne qui utilise plusieurs profils simultanément, et nous devons ensuite faire correspondre ces différentes identités, ces identités en ligne, à une identité réelle.

Frank Caputo: Combien de temps tout cela prend-il?

Mathias Van Laer: L'analyse médico-légale numérique d'un ordinateur peut prendre plusieurs mois. Cela ne fait pas partie de l'enquête sur le terrain. Cela dépend des ressources et des capacités. Cela dépend du contenu, de la taille de l'ordinateur et du nombre d'appareils qui ont été saisis à des fins d'enquête. Plusieurs facteurs sont en jeu.

Frank Caputo: À partir de là, les métadonnées sont-elles utiles dans les enquêtes en cours? C'est ma question, je crois.

Mathias Van Laer: Tout à fait. Je crois que, plus tôt, vous avez parlé du cas d'Amanda Todd. C'est l'un de ces cas où, sans la participation volontaire d'un important fournisseur de services électroniques, qui recueillait déjà les données et coopérait à notre enquête — et je crois qu'il était bien placé pour le faire —, nous n'aurions jamais pu identifier un suspect à l'étranger.

Le président: Merci, monsieur Caputo.

Madame Sodhi, allez-y, s'il vous plaît, vous avez six minutes.

Amandeep Sodhi (Brampton-Centre, Lib.): Merci, monsieur le président.

Merci à tous les témoins de comparaître devant le Comité aujourd'hui.

Ma première série de questions s'adresse à M. Brown. Pour commencer, je tiens à souhaiter un joyeux anniversaire à l'un des meilleurs maires que Brampton ait jamais eus.

Monsieur Brown, vous êtes l'un des dirigeants municipaux qui demandent le plus haut et fort des outils d'accès légal plus efficaces pour les services de police, étant donné que les régions de Brampton et de Peel font face à une augmentation de la criminalité, y compris l'extorsion et des activités criminelles organisées visant principalement la communauté sud-asiatique et ses entreprises.

L'an dernier, en décembre 2025, le conseil municipal de Brampton a adopté une motion approuvant l'envoi au gouvernement fédéral et aux gouvernements provinciaux d'une lettre demandant entre autres une intervention du gouvernement fédéral concernant l'accès aux preuves numériques, la création d'un groupe de travail dédié à la lutte contre l'extorsion et le crime organisé, le financement du soutien aux victimes et des activités de sensibilisation communautaires, ainsi que la mise en place d'un cadre officiel de partage de renseignements entre les organismes d'application de la loi fédéraux, provinciaux et municipaux.

À votre avis, quel sera l'effet des mesures prévues dans le projet de loi C-22, à l'échelle communautaire, pour nos électeurs, à Brampton?

Patrick Brown: Merci de la question, madame Sodhi.

Selon les organismes d'application de la loi, c'est un outil extrêmement important, qui fera toute la différence.

Hier, le chef de police Nish a fait une annonce importante. Dix-sept hommes ont été arrêtés pour extorsion avec violence. On m'a dit que l'enquête a nécessité un travail très difficile de la part de la police. Des policiers se sont mis en danger pour obliger ces criminels internationaux à répondre de leurs actes. On m'a dit que l'enquête aurait pu être effectuée en deux ou trois mois, plutôt que huit, et que les criminels ont fait plusieurs victimes pendant cette période, ce que le projet de loi aurait permis d'éviter.

Madame Sodhi, il ne s'agit pas seulement d'extorsion. Je peux vous parler de certains des crimes les plus ignobles commis dans la région. C'est un outil qui aurait pu les prévenir. Prenons un exemple que m'ont donné les agents de la police régionale de Peel. Récemment, deux personnes ont été victimes d'un cybercrime — une fraude à la cryptomonnaie —, et ces deux personnes innocentes se sont fait extorquer 1,6 million de dollars. Dans ce cas précis, les dispositions relatives à l'accès légal leur auraient permis d'identifier les responsables et de les poursuivre avant qu'ils puissent mettre la main sur cet argent.

Du côté de la traite des personnes, de l'exploitation des enfants et de l'extorsion, à mon avis, c'est un outil dont nos policiers ont désespérément besoin. Les chefs de police et les syndicats de policiers de tout le pays réclament cet outil et disent qu'ils en ont besoin; je ne comprends pas pourquoi il y a autant d'hésitation. Notre chef de police, envers qui j'ai la plus grande confiance — je crois que c'est l'un des meilleurs chefs de police du pays, et il était d'ailleurs chef des chefs, à une époque —, m'a assuré qu'il y a un équilibre. On vise précisément les infractions pour lesquelles il existe un motif raisonnable de croire qu'un crime a été commis. Le champ d'application n'est pas trop large. Pour ceux qui se préoccupent de l'atteinte à la vie privée, je crois que vous ne devez pas vous en faire, si vous ne menez pas d'activités criminelles.

J'ai une question: qu'en est-il du droit à la vie privée des victimes? Qu'en est-il du droit à ne pas voir son domicile criblé de balles? Et qu'en est-il du droit de ne pas voir ses enfants terrifiés?

Madame Sodhi, vous représentez la circonscription de Brampton. Je suis sûr que l'on vous fait part d'une foule de préoccupations. Des victimes m'appellent et me demandent ce que je vais faire, en tant que maire, pour les défendre.

L'une des choses que nous faisons, c'est d'implorer le gouvernement du Canada de mettre en place une loi actualisée en matière d'accès légal. Je remercie le gouvernement de l'avoir fait. Je sais que nos policiers dévoués sont reconnaissants de l'espoir et de l'aide qui s'en viennent. J'espère vraiment que l'adoption du projet de loi ne sera pas retardée.

● (1820)

Amandeep Sodhi: Merci de votre réponse, monsieur Brown.

Vous avez aussi collaboré dans ce dossier avec des maires et des chefs de police de tout le Canada et de la région de Peel, de Surrey à Edmonton en passant par Hamilton. Vos collègues des autres grandes villes partagent-ils votre opinion sur le projet de loi? À votre avis, dans quelle mesure les dirigeants municipaux canadiens s'accordent-ils à dire que le Parlement doit agir?

Patrick Brown: Je crois qu'il y a un consensus solide.

Avec le crime organisé, s'ils voient une échappatoire... Présentement, ils voient au Canada une échappatoire que les autres pays du Groupe des cinq ont éliminée. La police n'a pas un accès légal. Le phénomène va se reproduire partout dans le pays. Il va prendre de l'ampleur. Cela a peut-être commencé à Surrey et à Brampton, mais nous savons qu'il y a eu des cas à Calgary, à Edmonton et à Winnipeg. Des collègues, d'autres maires du pays, m'appellent et me disent que les mêmes incidents terrifiants dont je leur ai parlé se produisent maintenant dans leurs collectivités.

D'autres gangs et d'autres groupes du crime organisé commettront ces actes d'extorsion et ces activités criminelles odieuses, s'ils peuvent s'en tirer sans conséquence. La loi sur l'accès légal est un outil permettant aux policiers de s'assurer que ces criminels répondent de leurs actes. Ne faites pas de cadeau au crime organisé. N'hésitez pas et ne tardez pas. Présentement, 10 ou 15 villes canadiennes sont touchées, mais ce sera bientôt 100 villes si nous n'agissons pas. Nous avons déjà été trop lents à réagir, et c'est pourquoi les policiers se sont montrés si unis, clairs et éloquents quant à la nécessité du projet de loi.

Le président: Il vous reste 15 secondes.

Amandeep Sodhi: Merci, monsieur Brown.

Il me reste seulement 15 secondes, donc je vais vous remercier.

Patrick Brown: Merci.

Le président: Je suis désolé.

[*Français*]

Je cède maintenant la parole à Mme DeBellefeuille pour six minutes.

Claude DeBellefeuille: Je remercie beaucoup les témoins de s'être déplacés aujourd'hui pour venir comparaître devant nous.

Monsieur le commissaire, je ne sais pas si vous étiez connecté à la rencontre plus tôt, mais des représentants du Barreau du Québec sont venus exprimer leur désaccord sur la question du recours aux « motifs raisonnables de soupçonner » plutôt qu'aux « motifs raisonnables de croire », soit le seuil plus élevé, quand on rend une ordonnance.

Selon le bâtonnier du Québec, le fait d'avoir inscrit dans le projet de loi « motifs raisonnables de soupçonner », ça ne respecte pas l'esprit de la décision rendue par la Cour suprême. Toutefois, le ministère de la Justice et son ministre prétendent le contraire.

Pouvez-vous m'expliquer, ce que ça change pour les enquêteurs, l'utilisation des « motifs raisonnables de soupçonner » plutôt que des « motifs raisonnables de croire » lorsqu'il s'agit de rendre une ordonnance?

● (1825)

[*Traduction*]

le comm. Thomas Carrique: Je peux vous donner un exemple très précis en réponse à cette question importante.

Prenons le cas d'une personne disparue. L'enquête est lancée, et nous pensons qu'il pourrait y avoir eu des circonstances suspectes et que la personne disparue aurait pu être victime d'un homicide. Nous avons enregistré plusieurs appels entrants sur son téléphone. Ce sont les derniers appels connus. Cela ne nous donnerait pas un motif valable, au titre de la loi en vigueur, pour demander une ordonnance de communication. Toutefois, cela nous donnerait des motifs raisonnables de soupçonner qu'un crime a été commis. L'ordonnance de communication nous fournirait des informations sur l'abonné seulement, pas sur le contenu.

À mon avis, c'est un pas en avant important, qui nous aide à composer avec les défis liés aux lois et à la complexité des technologies et à secourir plus efficacement les victimes d'actes criminels.

[*Français*]

Claude DeBellefeuille: Si un amendement était proposé pour retirer les mots « motifs raisonnables de soupçonner » et les remplacer par « motifs raisonnables de croire », est-ce que ça handicaperait beaucoup votre travail d'enquête?

Actuellement, vous faites quand même de bonnes enquêtes. Vous avez les motifs raisonnables de croire.

Cela vous empêcherait-il de bien travailler?

Est-ce que ce serait dramatique pour vous si c'était retiré du projet de loi?

[*Traduction*]

le comm. Thomas Carrique: Les changements proposés au seuil ne nous empêcheront pas de faire notre travail. Dans les faits, ils nous permettront de mieux faire notre travail, de manière plus efficiente et plus rapide, et mener plus rapidement nos enquêtes, mais il nous faudra toujours un contrôle judiciaire et une autorisation judiciaire.

Comme M. le maire l'a dit, pour ce qui est de trouver l'équilibre approprié, je crois sincèrement que, s'il y a un motif raisonnable de soupçonner qu'un crime a eu lieu, cela justifie l'obtention des informations d'un abonné et constitue un motif raisonnable pour y accéder, ce qui représente un juste équilibre, compte tenu du contexte moderne.

[*Français*]

Claude DeBellefeuille: Monsieur le commissaire, depuis le début de l'étude relative au projet de loi, on sait que le Canada est le dernier du Groupe des cinq à déposer un projet de loi sur l'accès légal. Dans les autres pays du Groupe des cinq, de telles lois existent, dans certains cas depuis très longtemps.

Avez-vous des statistiques et des rapports qui pourraient établir un lien très étroit entre le fait d'avoir une loi sur l'accès légal et la diminution de la criminalité? Autrement dit, avez-vous des documents ou des statistiques qui montrent que la loi sur l'accès légal du Royaume-Uni, par exemple, a permis à ce pays d'arrêter plus de criminels et de faire baisser le taux de criminalité?

Avez-vous de la documentation là-dessus? Est-ce accessible?

[*Traduction*]

le comm. Thomas Carrique: C'est une excellente question. Je n'ai aucun document qui traite spécifiquement de la réduction de la criminalité ou de la gravité des crimes, mais nous avons d'innombrables exemples d'enquêtes qui n'ont pas pu progresser, y compris en lien avec la sécurité nationale et le risque de terrorisme, les homicides et la traite de personnes. Dans d'autres pays, ces enquêtes auraient été menées dans le cadre d'un dispositif d'accès légal approprié.

[*Français*]

Claude DeBellefeuille: On parle quand même d'un changement majeur pour le Canada. Il faut donc s'appuyer sur une analyse des statistiques. C'est ce que j'essaie de documenter. Je pense que le projet de loi C-22 a son utilité. Il donnerait de meilleurs outils aux forces de l'ordre en vue de combattre les criminels et le crime. Cependant, allons-nous trop loin ou pas assez loin? Nous essayons de voir quelle est la limite.

J'aime m'appuyer sur des données. Comme de telles lois existent ailleurs dans les pays du Groupe des cinq, par rapport auxquels le Canada aime se comparer, avez-vous pu accéder à de l'information qui vous permettrait de dire qu'une loi sur l'accès légal va améliorer la performance des enquêtes, données et résultats à l'appui?

● (1830)

[*Traduction*]

le comm. Thomas Carrique: Nous pourrions certainement chercher à savoir si des données spécifiques peuvent être utilisées. Il y a des exemples très concrets et convaincants, des cas où des personnes ont été victimes au Canada d'actes criminels, qui ont été évités, dans d'autres pays, des enquêtes complexes qui ont abouti, dans d'autres pays, alors que nous ne pouvons tout simplement pas jouer un rôle significatif dans les enquêtes sur la criminalité organisée internationale et transnationale. Nous sommes tout à fait disposés à vous donner des exemples pour vous aider à prendre une décision éclairée.

[*Français*]

Le président: Merci beaucoup, madame DeBellefeuille.

Monsieur Caputo, vous avez la parole pour cinq minutes.

[*Traduction*]

Frank Caputo: Je crois que c'est M. Lloyd.

[*Français*]

Le président: Monsieur Lloyd, vous avez la parole pour cinq minutes.

[*Traduction*]

Dane Lloyd: Merci, monsieur le président.

Merci aux témoins.

Joyeux anniversaire, monsieur Brown.

Vous avez dit quelque chose qui m'a frappé. Vous avez dit que les gens qui se préoccupent de l'atteinte à leur vie privée n'ont qu'à ne pas commettre de crime. Leur droit à la vie privée ne sera pas bafoué. Toutefois, nous avons appris une chose grâce à cette loi — nous l'avons vu avec les activités de piratage de Salt Typhoon, aux États-Unis — si nous laissons les arrêtés ministériels porter atteinte à l'intégrité des systèmes de chiffrement, nous risquons d'ouvrir des failles de sécurité que les pirates pourraient exploiter pour accéder aux renseignements de Canadiens innocents et respectueux de la loi.

Monsieur Brown, ma question s'adresse à vous; seriez-vous quand même en faveur de cette loi si vous saviez que nous créons une faille que des cybercriminels pourraient exploiter pour pirater vos informations personnelles et vos messages privés et s'en servir à des fins d'extorsion?

Patrick Brown: Je suis convaincu que le système mis en place et utilisé par les organismes d'application de la loi dans les autres pays du Groupe des cinq peut être reproduit ici.

Honnêtement, il y a beaucoup trop de victimes de crimes évitables. Je soutiens certainement le projet de loi. S'il y existe des mesures de protection supplémentaires pour prévenir les risques de piratage, je les adopte, mais si les entreprises technologiques peuvent prévenir ces risques grâce à leurs propres mesures de cybersécurité, dans d'autres pays, comme le Royaume-Uni et les États-Unis, je ne comprends pas pourquoi elles n'auraient pas la capacité de le faire au Canada.

Dane Lloyd: C'est précisément ce qui me préoccupe, monsieur Brown. Le projet de loi les empêche de créer ces mesures de sécurité... Il pourrait, en théorie, affaiblir leurs mesures de sécurité.

Je vais passer au commissaire Carrique.

C'est un projet de loi important. C'est quelque chose qui passionne les gens. J'ai parlé aux organismes d'application de la loi, et il est clair que nous devons y voir.

Le projet de loi revêt-il une telle importance, pour vous, que vous seriez en faveur des amendements visant à garantir aux Canadiens et aux entreprises que le chiffrement ne sera pas compromis à cause de ce projet de loi? Appuieriez-vous ces amendements, pour que ce soit très clair?

le comm. Thomas Carrique: Je soutiendrais certainement les amendements qui établissent clairement qu'il ne faut pas compromettre l'intégrité des systèmes, et je pense que cela peut se faire pendant l'élaboration du règlement.

Appelons un chat un chat. Les grandes entreprises technologiques ont complètement redéfini le monde tel que nous le connaissons. Les innovations et les progrès sont phénoménaux. Il doit y avoir un moyen, avec les centaines de millions de dollars que ces technologies génèrent chaque année, de protéger le chiffrement des Canadiens respectueux de la loi, tout en accédant à l'information des criminels qui s'en prennent aux Canadiens.

Dane Lloyd: Monsieur le commissaire, dites-vous au Comité que les organismes d'application de la loi doivent pouvoir décoder le chiffrement? C'est bien ce que vous dites au Comité, aujourd'hui?

le comm. Thomas Carrique: Ce que je dis, c'est que nous avons besoin d'une autorisation judiciaire pour accéder aux données chiffrées, et que nous avons cet accès légal, aujourd'hui. La loi en vigueur prévoit une autorisation judiciaire, quand elle est accordée par un juge de la cour supérieure provinciale, pour accéder aux communications privées. Nous n'avons pas les clés de chiffrement, c'est pourquoi nous devons utiliser des outils d'enquête embarqués.

Nous avons l'autorisation judiciaire, mais nous n'avons pas les moyens ou les mécanismes nécessaires, et cela fait toute la différence.

Dane Lloyd: Merci.

La question s'adresse peut-être à M. Van Laer, mais peut-être aussi au commissaire Carrique.

Après l'arrêt Bykovets de la Cour suprême, les équipes intégrées de lutte contre l'exploitation des enfants, en Alberta, ont dit que la rédaction des mandats et des ordonnances de communication était devenue un véritable cauchemar. Si nous ne savons pas s'il existe des attentes raisonnables en matière de protection de la vie privée concernant les adresses IP, il me semble que la partie 1 offre une solution adéquate faisant en sorte que les organismes d'application de la loi pourront accélérer la rédaction des mandats dont ils ont besoin pour demander des informations aux fournisseurs de services de télécommunications ou de courrier électronique.

Est-ce exact? Monsieur le commissaire, la partie 1 correspond-elle, en grande partie, à ce qui est nécessaire pour accélérer les enquêtes?

le comm. Thomas Carrique: Oui. Elle représente une bonne partie de ce qui est nécessaire pour accélérer les enquêtes; merci de l'avoir souligné, monsieur.

● (1835)

Dane Lloyd: Monsieur Van Laer.

Mathias Van Laer: Je dirais que notre problème... Nous n'avons pas vraiment de difficulté à obtenir des autorisations judiciaires, depuis la dernière décision de la cour. Nous devons d'abord comprendre d'où vient l'adresse IP, donc, si l'adresse IP est...

Je m'excuse. Allez-y.

Dane Lloyd: Monsieur Carrique, le commissaire à la protection de la vie privée a, à mon avis, présenté d'excellentes recommandations. Il a dit que, plutôt que d'avoir une période obligatoire d'un an pour la conservation des métadonnées, nous pourrions appliquer un critère de nécessité et de proportionnalité. Est-ce nécessaire et proportionnel?

Soutiendriez-vous cet amendement? Pensez-vous qu'il serait plus solide et qu'il offrirait une certaine tranquillité d'esprit aux Canadiens?

le comm. Thomas Carrique: Je ne vois pas le rapport, si les métadonnées n'étaient pas conservées pendant un an. Nous pourrions réaliser que c'est raisonnable et nécessaire une fois que les données ne seraient plus accessibles. Il faudrait que j'aie plus de détails sur cette recommandation pour vous donner une réponse réfléchie.

Dane Lloyd: Je comprends. Merci.

Le président: Merci, monsieur Lloyd.

Madame Sidhu, allez-y, s'il vous plaît, vous avez cinq minutes.

Sonia Sidhu (Brampton-Sud, Lib.): Merci, monsieur le président.

Merci aux membres du Comité de m'accorder du temps pour poser mes questions.

Merci, monsieur Brown. Joyeux anniversaire à un maire efficace.

Monsieur Brown, vous avez dit publiquement que les agents de police et les agents frontaliers ont besoin d'outils plus solides et d'un accès plus rapide et plus concret aux données sur les abonnés et les transmissions numériques, pour identifier les suspects avant qu'ils frappent. Nous savons que vous demandez depuis longtemps plus de soutien et des outils de balayage numérique pour les organismes d'application de la loi, pour assurer la sûreté et la sécurité de Brampton. Nos collectivités sont terrorisées par ces actes d'extorsion, et il y a aussi d'autres crimes.

À votre avis, comment le projet de loi C-22 concernant l'accès légal pour les organismes d'application de la loi peut-il donner aux organismes et aux services de police des outils plus modernes et susciter la confiance de la collectivité?

Patrick Brown: La dernière partie de votre question, la confiance, c'est très important. Présentement, on ressent un certain désespoir, parce que de nombreuses enquêtes sur des cas d'extorsion se sont enlisées. Les organismes d'application de la loi me répètent que, s'ils avaient un accès légal, ils pourraient trouver le responsable, mais que ces enquêtes s'enlisent.

Permettez-moi d'illustrer la chose, madame Sidhu. Si la police de Peel voyait un suspect... C'est un agent supérieur que m'a dit cela, pour expliquer pourquoi le projet de loi était nécessaire. Il m'a dit que, si vous voyez sur une séquence vidéo un suspect parler au téléphone, après qu'un crime a été commis, la police pourrait rédiger une ordonnance de communication pour une station cellulaire. À l'heure actuelle, il faudrait attendre au moins trois, quatre ou cinq semaines, voire 45 jours, pour obtenir cette ordonnance, et toutes les preuves essentielles seraient alors perdues. Les preuves seraient perdues. La vidéo serait perdue. D'autres crimes pourraient être commis, et les criminels échapperaient à la justice.

Voici un autre exemple; une des enquêtes que nous avons menées récemment a abouti, parce qu'ils avaient un accès légal aux États-Unis. L'un des criminels menait ses activités aux États-Unis, et ils ont pu l'attraper.

Les organismes d'application de la loi canadiens ne devraient pas dépendre des autres pays pour faire leur travail. Ils devraient avoir les mêmes outils modernes que les autres pays, avec les mêmes protections garanties par la Charte et des lois semblables. Si d'autres pays ont réussi à atteindre cet équilibre, je sais que le Canada en est capable. À mon avis, c'est une approche équilibrée dont nos policiers dévoués ont désespérément besoin.

Sonia Sidhu: Merci.

Nous savons que les activités criminelles se font de plus en plus en ligne, et nous avons de la difficulté à suivre le rythme avec les méthodes policières traditionnelles.

Croyez-vous que ce projet de loi fournira davantage d'outils pour lutter aussi contre la cybercriminalité?

Patrick Brown: Oui, tout à fait. La cybercriminalité, c'est la nouvelle forme de guerre numérique. Malheureusement, les organisations criminelles utilisent des technologies très sophistiquées. Si elles voient une échappatoire au Canada, elles vont en tirer profit.

C'est aussi un outil important pour prévenir la cybercriminalité. Le projet de loi comporte de nombreux aspects, à la demande des organismes d'application de la loi. C'est eux qui sont sur le terrain. Comme l'a dit M. Caputo, c'est leurs agents qui défoncent les portes, qui cherchent des preuves. Si les gens qui font ce travail très difficile — les agents des forces de l'ordre, qui mettent leur vie en danger — disent qu'ils ont besoin de cet outil, eh bien je fais confiance aux agentes et aux agents, et puisque cet outil a donné de bons résultats dans d'autres pays, il donnera de bons résultats ici.

● (1840)

Sonia Sidhu: Merci.

Hier, vous avez participé à la conférence de presse du chef Nish, sur les 17 hommes accusés d'extorsion. Nous avons tous vu la conférence de presse. Vous avez dit aujourd'hui que l'enquête avait pris huit mois, mais qu'elle aurait pu se conclure plus rapidement si les policiers avaient eu accès à des outils modernes.

Croyez-vous que les aînés, qui sont souvent la cible de fraudes et d'exploitation financière, pourraient en bénéficier?

Patrick Brown: Certainement.

Des aînés sont victimes de cybercrimes, même si vous en entendez moins parler que des cas d'extorsion très médiatisés survenus dans la région de Peel. Toutefois, pour des crimes de ce genre, je crois que c'est aussi un outil important pour les organismes d'application de la loi.

L'un des prochains témoins est le chef de police adjoint Nick Milinovich. Selon moi, il est l'un des plus brillants cerveaux du pays en ce qui concerne la technologie et l'application de la loi. Je crois que vous allez apprécier lui poser des questions techniques sur l'importance du projet de loi. Il pourra expliquer très précisément pourquoi il serait utile dans ces cas.

Sonia Sidhu: Monsieur le président, me reste-t-il encore un peu de temps?

Le président: Je suis désolé. Non, vous n'avez plus de temps.

Sonia Sidhu: Je tiens à remercier M. Brown de s'être joint à nous aujourd'hui, et de son engagement continu envers la sécurité publique, parce que c'est très important pour Brampton.

Merci.

Le président: Merci, madame Sidhu.

Madame DeBellefeuille, allez-y, vous avez deux minutes et demie.

[*Français*]

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur le commissaire, je voudrais discuter de la question de la conservation des métadonnées pendant un an.

Nous avons interpellé les fonctionnaires du ministère sur cette question. Ils ont fixé la période de conservation à un an de manière, semble-t-il, assez aléatoire. En Australie, c'est deux ans. J'ai entendu dire que, aux États-Unis, aucune période n'est fixée.

Une période d'un an, ça veut dire quoi, pour vous, comme enquêteur?

Nous avons eu des recommandations visant à fixer ça à 90 jours ou à 3 mois, par exemple, et de rendre ces périodes renouvelables au moyen d'une demande à cet effet, plutôt que d'enregistrer toutes les métadonnées des Canadiens et des Canadiennes pendant un an.

Si on réduisait cette période, avec certaines conditions, et qu'on vous permettait de refaire une demande de données, est-ce que vous pourriez vivre avec ça? Je ne comprends pas vraiment l'importance d'avoir une période de conservation d'un an.

Quel est votre point de vue de policier et d'enquêteur à ce sujet?

[*Traduction*]

le comm. Thomas Carrique: Merci.

À mon avis, un an est une période raisonnable, compte tenu du temps que prend chaque étapes d'une enquête pénale sur un crime grave ou complexe. Présentement, le Code criminel nous permet d'obtenir des ordonnances de préservation, qui limitent la durée de conservation des données connues à 90 jours. Toutefois, il faut plus de 90 jours pour conclure une enquête. Il nous sera impossible de savoir ce que nous avons besoin de savoir avant que les métadonnées ne soient plus accessibles.

Si j'ai bien compris le libellé du projet de loi, nous pourrons revoir la loi tard. À ce moment-là, il pourrait être approprié de déterminer si le délai prévu — moins d'un an — dans la version actuelle est suffisant.

[*Français*]

Claude DeBellefeuille: Monsieur le commissaire, il y a quand même beaucoup de témoins qui disent que, un an, c'est trop. Pour certains, nous devrions limiter la période de conservation des données et demander plus de renouvellements par voie judiciaire, par exemple.

Si on garde les métadonnées de tous les Canadiens et de toutes les Canadiennes, c'est quand même beaucoup de données, et ça ouvre une porte pour les criminels. Ils pourront alors voler ces données. C'est ce que nous disent aussi les entreprises.

Qu'en pensez-vous?

[*Traduction*]

le comm. Thomas Carrique: Je ne vois pas comment cela pourrait compromettre les systèmes et rendre les gens plus vulnérables aux actes criminels. D'après ce que j'ai compris, les métadonnées que nous voulons conserver pendant un an sont très spécifiques; elles concernent la date, l'heure, la durée et l'origine de la transmission. Il ne s'agit pas de contenu comme les courriels, les historiques de navigation ou les activités sur les médias sociaux. Pour ces métadonnées de base, pour le strict minimum qui pourrait faciliter les enquêtes complexes, nous aurions tout de même besoin d'une autorisation judiciaire.

Du point de vue de la police, je crois que c'est une période raisonnable.

● (1845)

[*Français*]

Le président: Merci, monsieur Carrique.

Monsieur Caputo, vous avez la parole pour cinq minutes.

[*Traduction*]

Frank Caputo: J'aimerais poursuivre dans la même veine que Mme DeBellefeuille, monsieur Van Laer, et connaître votre opinion sur les métadonnées et les délais. J'ai l'impression que le Comité ne comprend pas encore bien comment les métadonnées aident les enquêtes.

Vous me suivez, jusqu'ici?

Mathias Van Laer: Je crois que oui.

Frank Caputo: Qu'avez-vous à dire là-dessus? Dans quelles situations auriez-vous besoin de conserver les métadonnées pendant seulement 30, 60 ou 90 jours ou pendant un an? Auriez-vous un scénario en tête? Selon le projet de loi, vous devez conserver les métadonnées pendant un an. C'est une période de conservation arbitraire. Pourquoi un an?

Voici ce que j'essaie de comprendre; d'après l'expérience que vous avez acquise au cours de milliers d'enquêtes, combien de temps faut-il conserver les données?

Mathias Van Laer: C'est une question difficile. Si les enquêtes n'ont pas pu être menées, parce que les données avaient expiré, par exemple, nous ne saurions pas jusqu'où nous aurions pu aller si les données avaient été disponibles dès le départ.

Frank Caputo: Vous arrive-t-il souvent de déplorer l'absence de données, dans vos enquêtes?

Mathias Van Laer: Malheureusement, en raison d'un grand nombre de facteurs, cela arrive assez souvent, en ce moment, puisqu'il y a de nombreux retards dans le processus et qu'il faut parfois beaucoup de temps pour ouvrir une simple enquête. Dès le début, nous devons avoir accès aux informations sur l'abonné, par exemple. Si un fournisseur de services électroniques ou de services Internet n'est pas tenu de conserver ces données pendant une période donnée, nous risquons de devoir fermer le dossier avant même de commencer l'enquête.

Frank Caputo: Pouvez-vous nous donner un échéancier? D'après votre expérience, avez-vous un chiffre en tête, si vous dites: « Écoutez, présentement, les fournisseurs de services électroniques conservent ces données pendant 90 jours, et cela nous empêche souvent de mener nos enquêtes »?

Mathias Van Laer: Je ne sais pas si je peux vous donner un chiffre précis, autre que, comme vous l'avez dit, un chiffre fondé sur mon expérience. Malheureusement, j'ai déjà dû clore des enquêtes parce que les données avaient expiré. Il ne faut pas oublier d'où viennent les données. Le temps que les informations venant d'autres pays parviennent aux autorités canadiennes, sans parler des autorités provinciales, puis municipales, le délai peut expirer très rapidement.

Je ne suis pas ici pour vous donner un chiffre. Je suis simplement ici pour vous dire qu'un échéancier est essentiel.

Frank Caputo: D'accord.

Monsieur Carrique, vous avez longuement, et avec beaucoup de passion, insisté sur la nécessité du projet de loi. Ayant moi-même travaillé pour la poursuite, je le comprends. Je crois que ce que j'aimerais surtout savoir... et M. Brown peut lui aussi répondre à ma question. C'est un projet de loi important, mais il est tout aussi important de bien faire les choses — par exemple, faire la distinction entre « les motifs raisonnables de soupçonner » et les « motifs raisonnables de croire ». Seriez-vous d'accord pour dire que c'est complexe?

Par exemple, nous ne pouvons même pas nous entendre sur la période de conservation des métadonnées. Nous allons devoir, à un moment donné, examiner sérieusement la question et régler cela une bonne fois pour toutes. Je ne crois pas qu'il y ait place à l'erreur, ici. J'ai l'impression que les choses se sont faites dans la précipitation. M. Brown a dit « hésiter ». J'ai déjà passé des nuits à regarder le plafond, quand nos enquêtes ne nous permettaient pas de démasquer la personne derrière l'ordinateur. C'est frustrant. En même temps, en tant que parlementaires, nous devons nous assurer de bien faire les choses.

Qu'en dites-vous, tous les deux?

le comm. Thomas Carrique: Monsieur Caputo, je sais que vous comprenez, parce que vous avez déjà été procureur. Il est important de faire les choses correctement. À mon avis, nous ne pouvons pas perdre notre temps sur des choses qui ne sont pas vraiment importantes ou qui ne sont pas particulièrement pertinentes, comme débattre de la période de conservation de trois, six, neuf ou douze mois. Il faut bien commencer quelque part.

Je peux vous dire que, en 1996, quand j'étais un jeune agent détective, je faisais partie d'un groupe qui relevait du Service de renseignements criminels de l'Ontario, et j'avais signalé que nous étions gênés par l'avancée de la technologie par rapport aux lois désuètes. Trente ans plus tard, il n'y a eu aucun changement important. En 2002, l'Association canadienne des chefs de police a présenté au gouvernement fédéral la première d'une longue série de résolutions. Depuis, il n'y a eu aucun changement majeur.

Voici ma question: combien de temps faudra-t-il pour trouver une solution appropriée et combien d'autres victimes subiront des préjudices pendant ce temps-là?

● (1850)

Frank Caputo: Allez-y.

Patrick Brown: J'ajouterais que, selon moi, le libellé actuel du projet de loi tient au fait que l'on craignait que la Loi visant une sécurité rigoureuse à la frontière, la première version de celle-ci, aille trop loin. On voulait cibler plus précisément la criminalité. Je crois que le projet de loi vise justement à faire une pause et à proposer une nouvelle loi axée sur la criminalité. Du moins, c'est ce que m'ont dit les policiers locaux de Peel, qui ont été consultés au sujet du projet de loi.

Le président: Désolé de vous interrompre, monsieur Caputo et tout le monde.

Nous allons passer à M. Ramsay; allez-y, s'il vous plaît, vous avez cinq minutes.

[*Français*]

Jacques Ramsay: D'abord, je veux remercier les trois témoins.

Ils ont été très éloquents. J'avais plusieurs questions, et ils y ont répondu. Cependant, j'aimerais revenir sur une de ces questions pour bien clarifier les choses.

Il y a cette impression selon laquelle on est en train de se presser et que tout est un peu improvisé. Je pense que vous avez tous bien démontré que les dispositions du projet de loi sont plutôt réfléchies et qu'elles répondent à des impératifs très précis.

On veut souvent donner l'impression que le gouvernement s'est lancé dans une chasse à toutes sortes d'informations concernant les métadonnées. Or, je pense que c'est important de préciser une chose. À ma connaissance, les métadonnées visées par le projet de loi sont les suivantes:

[*Traduction*]

Les données de transmission Internet, les données de signalisation des stations, les données de signalisation pour les appels VoIP et les données de télémétrie des fabricants automobiles.

[*Français*]

Ce n'est rien de plus que ça. C'est précis. Je pense qu'au lieu de nous quereller, nous devrions reconnaître que le projet de loi C-22 vient justement clarifier l'étendue des données et empêcher une chasse aux sorcières.

J'aimerais avoir votre opinion là-dessus, monsieur le commissaire.

[*Traduction*]

le comm. Thomas Carrique: Merci beaucoup, monsieur le député. C'est avec plaisir que je vais vous donner mon opinion.

Je suis d'accord avec vous. C'est très précis. J'ai dit qu'il s'agissait du strict minimum d'information qui pourrait aider les enquêtes. Il n'est pas question ici d'aller à la pêche. Nous aurions tout de même besoin d'une autorisation judiciaire pour accéder aux métadonnées. Je suis tout à fait d'accord avec vos observations.

[*Français*]

Jacques Ramsay: Je suis très heureux d'entendre ça.

Un des témoins du Barreau du Québec a même semblé prétendre qu'avec l'adresse IP, on pouvait avoir accès à nos rêves. C'est un peu une extrapolation. C'est un peu n'importe quoi. L'adresse IP demeure une information de base qui va permettre aux policiers, avec un mandat, d'aller chercher l'information dont ils ont besoin.

L'autre point dont nous avons discuté, c'est la fameuse période de trois mois, qui serait peut-être insuffisante. Ce que j'ai compris de vos témoignages à tous les trois, c'est que les enquêtes débutent souvent alors que les crimes ont déjà été commis et qu'on ne peut pas savoir à l'avance de quelle information on va avoir besoin. Alors, on ne peut pas dire qu'on va garder juste un petit bout d'information en particulier parce qu'on va juste avoir besoin de ça. Ce n'est pas comme ça que ça marche.

Monsieur Van Laer, qu'en pensez-vous?

Mathias Van Laer: Je vous remercie de votre question.

Je suis d'accord avec vous.

Pour répondre à votre première question, j'aimerais faire des commentaires au sujet de l'adresse IP, si vous me le permettez. Vous avez tout à fait raison: on n'a pas accès aux rêves de tout un chacun par l'entremise d'une adresse IP. Donc, je suis content que ce soit retenu comme un facteur. Il est important que les gens ici, autour de la table, puissent développer des lois basées sur des activités ou des processus réels, c'est-à-dire des choses possibles. Il est impossible pour quiconque de pouvoir identifier quelqu'un à partir d'une adresse IP sans passer par un processus judiciaire. Donc, ça, c'est important.

Pour répondre à votre deuxième question, je dirais que oui.

J'espère que ça répond à vos questions.

Jacques Ramsay: Ma troisième question porte sur la raison de « croire » comparativement à la raison de « soupçonner ».

On comprend bien que, dans ce cas-ci, on parle d'une raison de soupçonner quelqu'un, parce qu'on va chercher des informations qui ne serviront pas de preuve en tant que telle. Une adresse IP, ou une adresse télémétrique, ce n'est pas une preuve pour inculper quelqu'un ou le déclarer coupable. Alors, c'est pour ça que le législateur a souhaité une norme juridique importante et reconnue, qui est la raison de « soupçonner » plutôt que la raison de « croire ».

Commissaire Carrique, qu'avez-vous à dire là-dessus?

● (1855)

[*Traduction*]

le comm. Thomas Carrique: Je suis d'accord. Comme je l'ai dit plus tôt, les motifs raisonnables de soupçonner sont la norme appropriée.

Comparons cela à l'époque des lignes téléphoniques fixes. Vous consultiez un bottin téléphonique pour chercher le nom d'une personne et vous trouviez son numéro de téléphone, et pas seulement son numéro de téléphone, son adresse aussi. Les bottins téléphoniques d'autrefois contenaient beaucoup plus d'informations personnelles qu'aujourd'hui; il faut maintenant avoir des motifs raisonnables de soupçonner qu'un crime a été commis pour obtenir l'adresse IP et ouvrir l'enquête. Vous aurez alors besoin de preuves plus solides, afin d'avoir des motifs raisonnables de porter des accusations.

[*Français*]

Le président: Je vous remercie beaucoup de ces échanges, monsieur Ramsay. Ça nous amène au terme de cette heure de discussion importante.

Nous remercions les trois témoins de leur temps et de la qualité de leurs interventions. Nous leur souhaitons une bonne fin de journée.

Pour les autres, nous allons suspendre la séance pendant quelques minutes.

● (1855)

_____(Pause)_____

● (1900)

Le président: Nous reprenons la séance.

Je souhaite un bon retour aux députés et je dis bonjour à tous les témoins.

Nous reprenons la séance en souhaitant la bienvenue à nos distingués invités: l'Association canadienne des télécommunications, représentée par M. Eric Smith; l'Ontario Child Sexual Exploitation Investigators Association, représentée par Andrew Ullock et Lisa Henderson, qui participent tous deux par vidéoconférence; la Peel Regional Police, représentée par M. Nick Milinovich; et Murray Rankin, un collègue très estimé dont nous nous ennuyons depuis très longtemps et que nous avons la chance de revoir aujourd'hui parmi nous à titre personnel.

Nous allons commencer par écouter une intervention de cinq minutes par personne.

Monsieur Smith, vous avez la parole.

● (1905)

[*Traduction*]

Eric Smith (vice-président principal, Association canadienne des télécommunications): Merci, monsieur le président, et merci aux membres du Comité, de me donner l'occasion de comparaître devant vous, aujourd'hui, au nom de l'Association canadienne des télécommunications.

Notre association s'est engagée à bâtir un avenir meilleur pour les Canadiens grâce à la connectivité. Nos membres comprennent des fournisseurs de services, des fabricants et d'autres organisations qui investissent dans les réseaux de télécommunications de classe mondiale du Canada, les bâtissent, les entretiennent et les exploitent.

J'ai écouté les discussions du Comité, et je dirais qu'il y a clairement un large consensus sur deux principes importants. Premièrement, le droit des Canadiens à la protection de la vie privée doit être protégé. Deuxièmement, les organismes d'application de la loi et les agences de sécurité nationale doivent avoir accès aux informations par des moyens légaux, pour soutenir les enquêtes légitimes et protéger la sécurité publique.

La question centrale n'est donc pas de savoir si ces objectifs ont de l'importance; c'est de savoir comment bien les équilibrer. Cet équilibre est essentiel, parce que les Canadiens, qui utilisent chaque jour des services numériques, s'attendent à ce que leurs informations personnelles soient traitées de manière sécuritaire et que l'accès à ces informations s'effectuera dans un cadre juridique clair, contrôlé et proportionné.

Nous apprécions que le gouvernement ait fait l'effort de consulter les parties prenantes et qu'il ait amélioré le projet de loi C-22 par rapport aux propositions antérieures contenues dans le projet de loi C-2. Je tiens à préciser que nous ne sommes pas contre le projet de loi. Toutefois, nous avons encore quelques préoccupations, que nous avons énumérées dans le mémoire écrit présenté au Comité. Je vais parler de trois d'entre elles.

L'un des points qui n'a pas encore été abordé concerne la partie 1 et le fait que les fournisseurs doivent répondre dans un délai de 24 heures à un ordre de confirmer la fourniture de services. Même si la plupart des fournisseurs de services ont prévu des processus pour gérer les demandes urgentes des organismes d'application de la loi, il n'est ni pratique ni réaliste de traiter tous les ordres de confirmer la fourniture de services avec le même niveau d'urgence, en n'accordant que 24 heures pour répondre.

Le nombre de demandes, la complexité des recherches et le fait que le personnel de certains fournisseurs de services n'est pas disponible 24 heures sur 24, sept jours sur sept, font qu'il est pratiquement impossible d'assurer un délai de réponse de 24 heures dans tous les cas. Un délai de trois jours ouvrables au moins serait plus raisonnable et serait approprié dans la plupart des cas; cela n'empêcherait pas les fournisseurs de services de répondre aux demandes réellement urgentes dans un délai plus court, comme ils le font actuellement.

L'autre élément préoccupant, c'est l'obligation de conserver des catégories générales de métadonnées pendant une période pouvant aller jusqu'à un an. Des témoins précédents vous ont déjà parlé des préoccupations en matière de protection de la vie privée que cela soulève. Nous nous préoccupons également des risques liés à la sécurité et du manque de garde-fous pour encadrer l'utilisation des métadonnées. Les dispositions sur les métadonnées du projet de loi C-22 devraient soit être supprimées, soit être grandement restreintes, en ce qui concerne tant la période de conservation que l'objectif.

Pour finir, il y a la question du remboursement des coûts importants que suppose la fourniture de services d'accès légal. Ce sont des outils et des services imposés par l'État, à l'usage exclusif des organismes d'application de la loi et des agences de sécurité, qui ne font pas partie des activités commerciales normales.

Lors d'une précédente consultation gouvernementale sur l'accès légal, des organismes d'application de la loi ont dit que les fournisseurs de services de communication « doivent être en mesure de recouvrer les dépenses raisonnables engagées pour donner suite à une ordonnance du tribunal ».

De plus, l'un des principes clés du Comité consultatif sur l'accès légal, créé par la GRC et le SCRS, est son engagement envers un modèle d'indemnisation juste qui n'entraîne pas de coûts. Encore une fois, je cite et je traduis:

> La communauté de l'accès légal reconnaît que les fournisseurs de services de télécommunications sont des entreprises privées ou semi-privées qui méritent de recevoir une indemnisation juste pour les efforts qu'elles consacrent à la conception, à l'entretien et au fonctionnement de capacités qui ne font pas partie de leurs processus opérationnels habituels.

D'autres pays, comme le Royaume-Uni, reconnaissent ces réalités économiques et remboursent aux fournisseurs de services de télécommunications le capital et les coûts d'exploitation liés au développement des capacités d'interception et à la présentation des données de communications. Ce concept devrait être inclus dans le projet de loi C-22.

Le remboursement des fournisseurs de services reflète la philosophie qui sous-tend le droit britannique, c'est-à-dire que, même si les entreprises privées ont l'obligation légale de contribuer à l'exécution de mandats, il ne faut pas s'attendre à ce qu'elles agissent bénévolement en tant qu'organe de l'État. Le financement gouvernemental aide aussi à assurer l'équité et la compétitivité du marché, atténue les répercussions financières sur les petites entreprises, permet de surveiller la qualité, les normes et le caractère sécuritaire des capacités d'interception et protège les citoyens contre une augmentation de leurs factures mensuelles visant à payer l'infrastructure d'enquête des organismes d'application de la loi.

Pour finir, nous savons que le cadre canadien sur l'accès légal doit être mis à jour. Grâce à des améliorations ciblées, le projet de loi C-22 fournira un cadre conciliant les intérêts liés à la protection de la vie privée et à la sécurité publique, de manière proportionnée et responsable, et qui ne répercute pas les coûts sur les consommateurs canadiens.

Merci. Je suis tout à fait disposé à répondre à vos questions.

[*Français*]

Le président: Merci, monsieur Smith.

Monsieur Ullock, vous avez la parole pour cinq minutes.

● (1910)

[*Traduction*]

Andrew Ullock (président du conseil d'administration, Ontario Child Sexual Exploitation Investigators Association): Bonsoir.

Merci de donner à l'Ontario Child Sexual Exploitation Investigators Association, l'OCSEIA, l'occasion de donner son avis sur le projet de loi C-22. L'OCSEIA compte des agents de police, d'anciens procureurs de la Couronne et des intervenants du secteur privé, qui collaborent pour soutenir ceux qui travaillent à tirer les enfants des griffes des agresseurs sexuels d'enfants en ligne.

Je m'appelle Andrew Ullock et je suis président du conseil d'administration de l'OCSEIA, à titre bénévole. J'ai 28 ans d'expérience en tant qu'agent de police, dont 14 ans dans le domaine de l'exploitation des enfants en ligne. J'ai travaillé en tant qu'enquêteur et superviseur d'agents de police, dans ce domaine.

Mme Lisa Henderson, membre elle aussi du conseil d'administration de l'OCSEIA, se joint à moi; elle a récemment pris sa retraite après 30 ans de service en tant que procureure de la Couronne. Du début des années 2000 jusqu'à sa retraite, Mme Henderson a été à la fois présidente du groupe de travail du procureur général sur les cybercrimes visant les enfants et coordonnatrice provinciale de la Couronne pour la stratégie provinciale de l'Ontario pour lutter contre la cybercriminalité visant les enfants.

La loi doit trouver un juste équilibre entre la protection de la vie privée et la protection du public contre la criminalité. La technologie évolue, et il est de plus en plus difficile de trouver cet équilibre. L'un des principes fondamentaux du droit pénal, au Canada, c'est que le fardeau de la preuve incombe à l'État, c'est-à-dire ses agents d'application de la loi. L'État doit établir hors de tout doute raisonnable qu'une personne est coupable d'un crime, et c'est une mesure de protection qui ne peut être compromise. Cela étant, si les organismes d'application de la loi ont le fardeau de respecter ce seuil nécessairement élevé, la loi devrait prévoir des moyens raisonnables leur permettant d'atteindre cet objectif.

Depuis la création d'Internet, la loi n'a guère évolué en ce qui concerne la manière dont la police recueille des preuves d'infractions criminelles, que ce soit en ligne ou à partir de données informatiques stockées sur des appareils. Sans mises à jour parlementaires, les tribunaux doivent s'adapter en comblant ce vide juridique par une mosaïque de décisions, qui peuvent prêter à confusion, être incohérentes et se chevaucher. Cette mosaïque correspond à ce que l'OCSEIA qualifie d'inflation juridique, c'est-à-dire que le nombre d'étapes que la police doit franchir et le nombre d'autorisations qu'elle doit obtenir pour mener à bien une enquête continuent d'augmenter, mais ne diminuent jamais.

Le temps est une ressource limitée pour les organismes d'application de la loi. Un policier ne peut pas travailler plus d'un certain nombre d'heures par année. Puisqu'il faut de plus en plus de temps pour mener une enquête, le nombre d'enquêtes que la police peut mener diminue. Les lois sur la protection de la vie privée ne devraient pas créer des obstacles ou multiplier les barrières impossibles à surmonter pour les policiers. Des limites raisonnables aux pouvoirs d'enquête de la police protègent la vie privée et la dignité des citoyens; des limites déraisonnables protègent les criminels.

Le projet de loi C-22 a donné lieu à de nombreuses discussions sur le droit à la vie privée des Canadiens. L'OCSEIA reconnaît que c'est un débat important et apprécie les contributions des défenseurs du droit à la vie privée. Toutefois, au sujet de la protection de la vie privée, l'OCSEIA veut s'assurer qu'il s'agit d'une discussion de fond qui tient compte de toutes les facettes du problème.

Derrière chaque statistique ou chaque rapport de police sur l'exploitation des enfants en ligne se trouve un enfant qui a été victime d'abus terribles de la part d'un prédateur. Ces enfants méritent, eux aussi, que l'on tienne compte de leur droit à la vie privée, dans ce débat, puisque c'est leur vie privée qui est atteinte, et pour toujours, de la manière la plus sordide qui soit. Une fois qu'un délinquant prend une photo à caractère sexuel d'un enfant, celle-ci sera à tout jamais sur Internet. À partir de ce moment-là, le droit à la protection de la vie privée de l'enfant sera bafoué chaque fois qu'un nouveau délinquant consulte ou partage l'image.

En tant que société, la meilleure façon de réagir à ces atteintes à la vie privée est de retrouver et de traduire en justice ceux qui, par plaisir, exploitent les enfants. Pour cela, les organismes d'application de la loi ont besoin des bons outils. L'OCSEIA estime qu'il existe de nombreux outils pertinents que l'on peut utiliser pour y parvenir.

Les organismes d'application de la loi canadiens ne devraient pas avoir à conclure un traité d'entraide juridique pour obtenir les données de contenu auprès d'un fournisseur de services en ligne qui a une présence physique au Canada, du simple fait qu'il s'agit d'une entreprise internationale, alors qu'ils pourraient utiliser une ordonnance de communication.

Les organismes d'application de la loi ne devraient pas avoir à obtenir un deuxième mandat de perquisition inutile pour analyser un ordinateur, simplement parce que l'appareil a été saisi dans la main ou la poche d'une personne lors de l'exécution d'un mandat de perquisition d'un domicile, qui autorisait déjà la saisie et l'analyse de tout appareil trouvé sur les lieux.

Les organismes d'application de la loi ne devraient pas avoir à obtenir une autorisation judiciaire préalable pour saisir une adresse IP visible par des millions d'autres utilisateurs sur un réseau de partage de fichiers en pair-à-pair.

Les organismes d'application de la loi devraient pouvoir, grâce à une autorisation judiciaire préalable, obtenir des informations sur un abonné à Internet plus de 30 jours après qu'un délinquant a exploité un enfant, de façon à pouvoir lui mettre le grappin dessus et, dans certains cas, secourir un enfant victime d'abus.

Pour être jugés raisonnables, les pouvoirs d'enquête conférés aux organismes d'application de la loi ne doivent pas porter atteinte de manière déraisonnable à la vie privée de citoyens. Nous sommes tous d'accord avec cela. Toutefois, ces pouvoirs doivent aussi donner les résultats escomptés. Il n'est pas raisonnable, au quart du XXIe siècle, de s'attendre à ce que les forces de l'ordre protègent la société contre la criminalité en s'appuyant sur des lois relatives aux perquisitions et aux saisies rédigées au XIXe et au XXe siècles.

● (1915)

L'OCSEIA croit que nos commentaires et nos recommandations aideront le Parlement à trouver le juste équilibre.

Nous sommes prêts à répondre aux questions du Comité.

Le président: Merci, monsieur Ullock.

Monsieur Milinovich, allez-y, s'il vous plaît, vous avez cinq minutes.

Chef adjoint Nick Milinovich (chef de police adjoint, Peel Regional Police): Monsieur le président, membres du Comité, merci de me donner l'occasion de vous parler du projet de loi C-22, Loi concernant l'accès légal. Cette discussion est à l'intersection de deux priorités très importantes pour les Canadiens, à savoir soit la sécurité publique et la protection des renseignements personnels. En tant que chefs de police, nous soutenons les deux.

La criminalité a beaucoup changé au cours de la dernière décennie. Les groupes du crime organisé, les extorqueurs, les trafiquants d'êtres humains, les réseaux de fraude et, comme nous venons de l'entendre, les délinquants qui exploitent des enfants commettent principalement leurs crimes sur des plateformes numériques, tandis que la plupart des pouvoirs en matière d'enquêtes ont été conçus pour un environnement technologique très différent.

L'objectif du projet de loi C-22, selon nous, n'est pas d'affaiblir les mesures de protection des renseignements personnels ni d'étendre l'autorité du gouvernement sans aucune surveillance. Il vise à s'assurer que les enquêteurs puissent continuer d'obtenir légalement des preuves essentielles dans des enquêtes sur des crimes graves tout en restant assujettis à une surveillance judiciaire, à des seuils juridiques et à l'exigence de rendre des comptes et de respecter les protections prévues dans la Charte.

Aujourd'hui, j'aimerais vous faire part du point de vue de nos intervenants de première ligne, de nos enquêteurs et notre collectivité, qui ont été très touchés par la criminalité. Ils sont concernés par ce sujet. En leur nom, je vous demande d'adopter rapidement le projet de loi C-22, Loi concernant l'accès légal.

Les lois actuelles qui régissent nos enquêtes ont été conçues avant l'ère numérique. Aujourd'hui, les criminels profitent activement de ce retard, dans les régions en pleine expansion et ailleurs, comme à Mississauga et à Brampton. Nous voyons une augmentation sans précédent des crimes commis au moyen des technologies.

Nos équipes se heurtent à des murs systémiques et artificiels. Nous voyons des menaces actives disparaître dans l'ombre du numérique, simplement parce que notre cadre juridique nous force à mener des enquêtes dans l'ère numérique complexe de 2026 munis d'outils analogiques désuets.

Hier, notre service a annoncé les résultats d'une des plus grandes enquêtes en matière d'extorsion menées dans notre collectivité. Tout a commencé par une menace envoyée par voie numérique à partir d'une plateforme chiffrée en novembre 2025. Si le projet de loi C-22 avait été adopté, à ce moment-là, notre enquête aurait été plus efficace et plus rapide et nous aurions pu mettre fin à ces menaces d'extorsion.

Dans la région de Peel — et partout au Canada —, les services de police luttent contre une augmentation très perturbatrice de l'extorsion, de la traite de personnes, de l'exploitation d'enfants et d'une foule d'autres crimes transnationaux. Presque tous ces crimes ont un modèle commun. Ils ont tous commencé par une communication numérique, un message chiffré et un profil en ligne ou une adresse IP anonyme, avant de prendre de l'ampleur et de se transformer en violence réelle dans nos rues, ce qui a des conséquences pour notre collectivité.

À l'heure actuelle, quand on reçoit une alerte numérique, il nous faut des semaines d'échanges bureaucratiques pour déterminer quelle entreprise de télécommunications ou quel fournisseur gère le compte suspect. Le temps vient à bout du casse-tête, la trace est effacée, des données ont été supprimées et des preuves ont été perdues. En réalité, les criminels continuent leurs activités et exploitent nos collectivités.

Je crois que le projet de loi C-22 propose les mesures nécessaires pour raccourcir de beaucoup la durée de nos enquêtes. Il nous permet de retrouver les suspects et de mettre fin à une série d'activités criminelles avant que la violence s'en mêle. Il nous permettra de prévenir la victimisation et la criminalité dans nos collectivités.

En tant que professionnels des forces de l'ordre, nous avons fait le serment de respecter la Charte canadienne des droits et libertés. Nous ne voulons pas de capacités de surveillance arbitraires dans notre collectivité. Le respect de la vie privée et la sécurité peuvent et doivent cohabiter, et je crois que le projet de loi C-22 a trouvé le parfait équilibre.

Comme je l'ai mentionné, nous avons récemment arrêté 17 personnes qui ciblaient la communauté des gens d'affaires sud-asiatiques. Encore une fois, nous menons cette enquête depuis sept mois, et elle est toujours en cours. Durant cette période, nous croyons que ce groupe a tiré 320 coups de feu dans notre collectivité. C'est plus de la moitié des tirs d'armes à feu illégales dans notre collectivité cette année.

Nous sommes très satisfaits de ces résultats, mais, comme je l'ai dit, je crois que l'enquête aurait pu se faire plus rapidement et plus efficacement et que les victimes auraient pu être moins nombreuses.

● (1920)

Encore une fois, cela vaut pour les enquêtes en matière d'extorsion, mais aussi pour des enquêtes sur des homicides, sur la sécurité nationale, sur la traite de personnes et, comme nous l'avons entendu, sur l'exploitation d'enfants, ainsi que sur toutes sortes d'autres crimes transnationaux dont nous commençons à être victimes, très localement, dans nos collectivités.

Un accès rapide à des preuves numériques doit être non négociable si nous voulons mieux trouver les victimes et éviter des préjudices communautaires. Je crois que le projet de loi C-22 offre les outils de surveillance précis, transparents et judiciaires dont nous avons besoin pour mieux faire notre travail. Nous vous demandons d'adopter ce projet de loi essentiel.

Merci. C'est avec plaisir que je répondrai à vos questions.

Le président: Merci, monsieur Milinovich.

[*Français*]

Monsieur Rankin, vous avez la parole pour cinq minutes.

L'hon. Murray Rankin (avocat, à titre personnel): Merci, monsieur le président.

Membres du Comité, je vous remercie beaucoup de m'avoir invité à comparaître aujourd'hui. Je suis heureux d'être ici pour discuter du projet de loi C-22.

C'est un texte législatif important, complexe et sensible. Il touche à la sécurité publique, à la protection de la vie privée, à la cybersécurité, à la Charte canadienne des droits et libertés et à la capacité réelle des policiers et des membres du Service canadien du renseignement de sécurité de faire leur travail dans un monde numérique.

Ce débat n'est pas simplement technique; il s'agit d'un débat de société. Comment protéger les Canadiennes et les Canadiens contre l'exploitation sexuelle des enfants, la fraude, l'extorsion, le terrorisme et l'espionnage, tout en protégeant les droits fondamentaux qui définissent notre démocratie? À mon avis, ces objectifs ne sont pas contradictoires, ils sont complémentaires. L'accès de l'État à l'information doit être légal, nécessaire, proportionné, clairement autorisé et assujetti à une reddition de comptes efficace.

J'ai été le premier président de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, et cette expérience m'a profondément marqué. Elle m'a appris deux choses. Premièrement, les organismes de sécurité et d'application de la loi ont besoin d'outils modernes. Deuxièmement, ces outils doivent être encadrés par une loi claire, par un organisme de surveillance indépendant et par le Parlement.

[*Traduction*]

C'est pour cette raison que je crois fermement que nous avons besoin d'un projet de loi sur l'accès légal. Le monde numérique a changé la nature des enquêtes. Les criminels, les États hostiles et les réseaux complexes se servent de technologies qui n'existaient tout simplement pas quand la plupart de nos outils d'enquête ont été conçus. Le Canada a désespérément besoin d'un cadre juridique moderne, mais ce cadre doit être canadien. Il doit respecter notre Charte, nos exigences de protection de la vie privée, être réaliste sur le plan technologique et être bien surveillé.

J'ai eu le plaisir d'apporter mon aide dans le cadre des consultations qui ont suivi le projet de loi C-2. J'ai rencontré individuellement des parties prenantes des secteurs de l'application de la loi, de la sécurité nationale, de l'industrie, de la société civile, des universités et de la protection de la vie privée. Selon moi, il a été très utile de les regrouper, ensuite, tous au même endroit. Les gens étaient parfois vivement en désaccord, mais le processus a été fructueux. Je crois que mon rapport reflète fidèlement la gamme des points de vue avec exactitude.

J'ai aussi été ravi de voir que la plupart de mes recommandations se sont retrouvées dans le projet de loi C-22. Le projet de loi est maintenant autonome. La demande d'information a été restreinte et est maintenant un ordre de confirmer la fourniture de services. Ce projet de loi accorde plus d'importance à la surveillance, à la transparence, à la cybersécurité et à l'examen parlementaire. Cela ne veut pas dire qu'il est parfait. Aucun projet de loi n'est parfait. Le ministre a dit qu'il était ouvert à des amendements, et je prends cela très au sérieux. En tant qu'ancien député, j'ai beaucoup de respect pour le travail des comités parlementaires comme le vôtre. C'est ici que les projets de loi peuvent être améliorés et rendus plus durables.

À mon humble avis, votre travail n'est pas de choisir entre la protection de la vie privée et la sécurité publique; c'est d'insister sur ces deux choses. Le projet de loi devrait préserver l'efficacité opérationnelle tout en protégeant la vie privée, les valeurs inscrites dans la Charte et la cybersécurité. Il devrait protéger les renseignements confidentiels, médicaux et très sensibles. Il devrait garantir que tout nouveau pouvoir conféré est utilisé adéquatement, par des responsables adéquatement formés, et il doit être soumis à un examen après un certain temps.

J'encouragerais surtout le Comité à porter attention à ces cinq aspects: la clarté de l'ordre de confirmer la fourniture de services, la définition de la vulnérabilité systémique, le rôle du commissaire au renseignement et de l'OSSNR, la transparence et les rapports annuels et un examen parlementaire obligatoire après trois ans.

Enfin, je crois que l'objectif de ce projet de loi doit être clairement exposé. L'accès de l'État à de l'information à des fins d'enquête doit être légal, nécessaire, proportionnel et assujetti à des exigences en matière d'autorisation et de reddition de comptes, conformément à la Charte et aux lois sur la vie privée du Canada.

Encore une fois, merci de m'avoir invité, monsieur le président. J'ai hâte de répondre à vos questions.

● (1925)

[*Français*]

Le président: Merci beaucoup, monsieur Rankin.

Madame Kirkland, je vous passe la parole pour six minutes.

[*Traduction*]

Rhonda Kirkland: Merci, monsieur le président.

Merci à vous tous d'être ici.

Je me dois de mentionner, encore une fois, que c'est beaucoup d'information en même temps. On va se noyer dans toute cette information. Il y a cinq témoins. J'aimerais pouvoir leur poser des questions sur chacune des déclarations liminaires, mais franchement, nous n'avons pas le temps, malheureusement.

Je sais que vous comprenez tous le rôle des membres de l'opposition, surtout vous, monsieur Rankin. Je vous remercie d'être ici. Vous avez été député de l'opposition pendant un certain nombre d'années, donc vous comprenez que, parfois, quand vous faites partie de l'opposition, on dirait que vous ne faites que vous opposer, alors que ce n'est pas le cas. Tous ceux parmi nous qui regardent très attentivement la situation veulent faire les choses comme il se doit. Ce qui m'inquiète, c'est que le rôle des députés de l'opposition est quelque peu minimisé, quand on veut faire avancer un peu trop vite le projet de loi. Des mots comme « hésiter » ont été utilisés, plus tôt, et je n'ai pas aimé cela, simplement parce que nous voulons examiner cela en profondeur. La situation mérite que l'on fasse les choses comme il se doit.

En 2012, un gouvernement conservateur a essayé de faire la même chose et a fini par reculer parce que le porte-parole libéral en matière de sécurité publique de l'époque s'y opposait fermement. Le projet de loi aujourd'hui en a fait un peu plus.

J'ai fait un long préambule, mais il y a tant de choses que j'aimerais examiner. Je sais que je peux vous poser à tous des questions en privé, mais cela empêcherait les Canadiens et les Québécois d'entendre ce qu'ils ont besoin d'entendre ouvertement et en public.

Monsieur Rankin, vous avez mentionné le processus que vous avez suivi et les tables rondes. Je suis très heureuse de vous voir ici. Je suis heureuse d'avoir reçu une version du rapport. Il est peut-être un peu caviardé, mais au moins, nous avons quelque chose. C'était une de mes demandes, donc je suis très heureuse de le voir ici.

Combien de temps le processus à cet égard a-t-il pris? Seriez-vous capable de dire combien d'heures environ?

L'hon. Murray Rankin: Merci beaucoup, madame Kirkland.

Merci d'avoir mentionné que j'ai fait partie de l'opposition et que c'est le rôle que j'ai eu à jouer. Je respecte beaucoup ce que vous avez dit sur le fait qu'il ne s'agit pas simplement de s'opposer, mais plutôt de faire des efforts pour faire les choses comme il se doit. C'est essentiel pour un projet de loi comme celui-ci.

Je pense qu'une occasion s'offre à nous, et cela commence par le rapport du Comité des parlementaires sur la sécurité nationale et le renseignement de 2025. Toutes les parties se sont réunies, pour ce rapport, afin de comprendre pourquoi l'accès légal était nécessaire. C'est un rapport mûrement réfléchi. Cela nous donne une ouverture.

Certaines personnes disent que c'est la septième fois que nous essayons, d'autres disent que c'est la neuvième. Vous avez mentionné une tentative des conservateurs. C'est seulement une parmi tant d'autres. Il est plus que temps. Vous avez entendu différents témoins. Je les ai écoutés nous expliquer qu'ils sont mal outillés pour composer avec le numérique et que cela nuit à leur travail.

Rhonda Kirkland: Excusez-moi. Je ne veux pas vous interrompre, mais mon temps est limité.

Vous avez parlé de tables rondes. Savez-vous combien de temps vous y avez passé...?

L'hon. Murray Rankin: J'y venais. Je vous dirais que j'y ai passé entre 20 et 30 heures. Ce n'est qu'une estimation.

● (1930)

Rhonda Kirkland: Donc, entre 20 et 30 heures.

L'hon. Murray Rankin: Nous avons eu des réunions distinctes avec chaque groupe de parties prenantes, puis nous avons eu une réunion de groupe.

Rhonda Kirkland: Excellent. De notre côté, le Comité aura entre 8 et 10 heures. J'adorerais avoir entre 20 et 30 heures pour comprendre pleinement la situation.

Je sais que vous allez sans doute revenir sur des choses que vous avez mentionnées. Selon vous, a-t-on soulevé des préoccupations importantes qui auraient pu être mieux traitées, ou examinées de plus près ou incluses dans le projet de loi final?

L'hon. Murray Rankin: Il a été question de ce que M. Smith a dit concernant l'indemnisation, et cela est reflété explicitement dans le projet de loi, pour ce qui est des fournisseurs non essentiels. On parle d'indemnités « appropriées ». Pour ce qui est des fournisseurs principaux, ce n'est pas clair. C'est un aspect qui mérite peut-être réflexion.

J'ai déjà dit ailleurs que les métadonnées ne nous préoccupaient pas vraiment. La conservation des données, évidemment, est une caractéristique importante, mais nous ne nous sommes pas attardés trop longtemps sur cette question.

Ce sont les deux choses qui me viennent à l'esprit.

Rhonda Kirkland: C'est intéressant que vous mentionniez cela, parce que ce sont les sujets qui ont entraîné le plus de questions et de témoignages, au Comité. Il y a une raison à cela. Quand il n'y a pas suffisamment d'information, nous avons plus de questions. Je vous remercie de l'avoir souligné.

Je sais que vous avez dit ailleurs qu'il n'a jamais été question de la période de conservation d'un an. Je pense que c'est ce qui préoccupe le plus les Canadiens, parce que nous ne parlons pas seulement des métadonnées des personnes malintentionnées. Nous parlons des métadonnées de tout le monde.

Pourriez-vous dire quelque chose à ce sujet, ou voulez-vous dire quelque chose à ce sujet?

L'hon. Murray Rankin: Je sais que le Comité comprend la différence entre le contenu et les métadonnées, et que les métadonnées donnent l'accès à l'information concernant le moment et l'endroit où un appel a été fait, qui était au bout du fil, et ainsi de suite. Par le passé, et actuellement, je crois, la période de conservation des métadonnées a énormément varié, donc je pense qu'il est intéressant et important de fixer une période — le projet de loi prévoit un an — parce que tout n'était vraiment pas uniforme. Les services de police m'ont dit pendant ces consultations qu'il était très difficile de s'entendre avec les différentes forces policières.

Je pense que les Canadiens doivent comprendre que cela s'est fait en Australie, où on parle de jusqu'à deux ans; au Royaume-Uni, où c'est jusqu'à un an; en France, où c'est jusqu'à un an; en Belgique, où c'est jusqu'à un an et en Suède, où on parle d'une période de 10 mois maximum. Il n'y a pas de durée idéale, mais je pense que, pour mener leurs enquêtes complexes, les services de police modernes auront besoin que les données soient conservées pendant une période raisonnable. Je ne sais pas si c'est un an ou 10 mois, mais c'est une période fixe.

Rhonda Kirkland: Merci. Cela répond à ma question.

Le président: Merci.

Excusez-moi, madame Kirkland, votre temps est écoulé.

Rhonda Kirkland: Vous voyez. C'est exactement ce que je disais. J'ai besoin de plus de temps avec vous.

Le président: Nous aimons toujours entendre ce que vous avez à dire.

C'est maintenant au tour de Mme Acan, qui a six minutes; allez-y.

Sima Acan: Je n'ai pas de préambule. C'est promis. Le temps est précieux.

Merci beaucoup d'être présent aujourd'hui, monsieur Milinovich. Je suis heureuse de vous voir.

Je vais poser ma question en revenant sur un commentaire de M. Baber. Il a dit que les organismes d'application de la loi pouvaient déjà obtenir un mandat de perquisition et de demander à Google de respecter les demandes d'information, et il a demandé si c'était bien cela.

Pourriez-vous expliquer les enjeux auxquels font face les organismes d'application de la loi à l'heure actuelle?

chef adj. Nick Milinovich: Je serais ravi de vous en parler, mais j'aurais besoin de beaucoup plus que six minutes pour le faire.

Dans les faits, si vous regardez le projet de loi sur l'accès légal, la dernière mise à jour d'envergure date d'avant la conception de Google. Si vous prenez notre mode de fonctionnement actuel, simplement dit, nous tardons à obtenir l'information. Nous ne sommes pas aussi efficaces que nous pourrions l'être et nous ne sommes certainement pas aussi efficaces que d'autres pays du Groupe des cinq. Nous sommes contraints par des lois désuètes, et cela doit changer.

C'est pour ainsi dire le fondement de toutes les enquêtes complexes que nous menons. Normalement, on commence par une ordonnance de communication, qui peut entraîner d'autres demandes d'autorisation judiciaire, mais nous attendons plus de temps qu'il faut pour les obtenir et elles ne sont pas suffisamment détaillées pour nous aider à nous acquitter de nos fonctions. Nous sommes dans une situation difficile.

Laissez-moi vous donner un exemple. Si nous étions témoins d'une extorsion, à Peel, que les enquêteurs vont sur le terrain, mènent leur enquête et découvrent qu'un commerce sur le coin de la rue a une vidéo de l'extorsion. On y voit la personne parler au cellulaire, et nous pourrions demander une ordonnance de communication pour cette station. Dans certaines administrations, on pourrait devoir attendre jusqu'à 30, 45, voire 50 jours avant d'obtenir les résultats. Pendant ce temps, nous avons perdu des preuves. Nous avons perdu la possibilité de prévenir d'autres crimes. Cela n'arrive pas tout le temps, mais c'est l'un des gros enjeux auxquels nous faisons face.

Nous avons la possibilité d'être plus efficaces dans nos enquêtes en améliorant la loi sur l'accès légal.

● (1935)

Sima Acan: J'ai appris que les gouvernements canadiens successifs essaient de faire adopter une loi sur l'accès légal depuis la fin des années 1990. Cela fait plus de 25 ans. Ça fait longtemps. Cela veut dire que le dossier de l'accès légal a été étudié ici pendant des heures et des heures au cours des 25 dernières années. Le projet de loi C-22 a aussi fait l'objet de nombreuses heures de consultation, et il est appuyé par un énoncé concernant la Charte qui explique son incidence sur les droits prévus dans la Charte, surtout ceux énoncés à l'article 8.

Dans l'optique des services policiers, diriez-vous que le projet de loi C-22 n'interfère pas avec l'article 8? Est-ce que des outils comme l'ordre de confirmer la fourniture de services respectent ces droits?

chef adj. Nick Milinovich: C'est difficile de commenter tous les scénarios, mais selon nous, le projet de loi C-22 actuel respecte la Charte. Si ce n'était pas le cas, je ne serais pas ici à vous demander de l'adopter. Outre la question du respect de la Charte, de la surveillance judiciaire et de l'examen, on pourrait pour d'autres raisons remettre en question l'authenticité du projet de loi et son respect de la vie privée. Je crois que c'est ce qui va se passer.

Pour en revenir à votre premier point, la dernière mise à jour d'envergure de la loi remonte au début des années 1990, soit avant Google et avant l'iPhone. C'est pour cette raison que je suis ici au nom de mon organisme et que je vous demande à genoux de l'aide pour protéger notre collectivité.

Sima Acan: Monsieur Milinovich, vous avez déjà travaillé sur le dossier de l'accès légal dans d'autres projets de loi et vous travaillez dans le domaine de l'application de la loi depuis très longtemps. Diriez-vous que, pour des enquêtes complexes, il est raisonnable de conserver des métadonnées jusqu'à un an, ou, comme il est indiqué dans le projet de loi, 12 mois?

Je sais que les sociétés technologiques suppriment souvent les données des abonnés plus rapidement.

chef adj. Nick Milinovich: C'est une excellente question.

J'aurais tendance à être d'accord avec M. Rankin. On doit fixer une période. Nous devons exiger que les gens conservent les métadonnées pendant un certain temps, parce que ce n'est pas comme si nous pouvions recueillir ces informations dès qu'un crime est commis. Les crimes, et surtout les crimes plus graves, ne font pas l'objet d'une limite de temps. Nous ne parlons pas d'un vol à l'étalage. Nous parlons de l'exploitation d'un enfant ou d'un crime transnational, et cette information peut devenir très précieuse pour les enquêteurs et la police.

Évidemment, je comprends que les gens soient inquiets, quand on parle de simples citoyens qui ne commettent aucun crime. Je comprends cela, mais, dans les faits, personne n'examinera les métadonnées de ces gens-là parce qu'ils ne font rien de répréhensible selon la loi. Quand il est question d'un criminel qui cible nos collectivités, pour nous, plus on conserve les métadonnées longtemps, mieux c'est.

Sima Acan: Pourriez-vous simplifier tout cela? Pourriez-vous nous expliquer comment ces données peuvent servir à résoudre rapidement une affaire d'extorsion ou, comme vous l'avez dit, d'exploitation sexuelle d'enfants?

chef adj. Nick Milinovich: Laissez-moi faire un parallèle. Tout le monde connaît les preuves médico-légales physiques. C'est quelque chose de bien accepté. Nous avons tous vu une émission de *CSI*. Je pense que la plupart des gens comprennent cela. Vous pouvez laisser des indices sur une scène de crime, qui peuvent être recueillis par la police et conservés pour toujours.

Nous avons effectué des arrestations des dizaines d'années après un crime parce que nous avons pu recueillir cette information et la conserver. Les preuves numériques sont très semblables à cela. C'est une empreinte. Pour nous, quand il est question d'enquêtes contemporaines ou de sécurité publique, ces preuves sont aussi importantes que les preuves médico-légales physiques.

Sima Acan: Je crois que mon temps est écoulé.

Le président: En effet.

C'est maintenant au tour de Mme Debellefeuille, qui a six minutes; allez-y.

[*Français*]

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

D'abord, monsieur Rankin, je veux vous remercier d'avoir parlé en français, parce que je ne sais pas si mes collègues anglophones auraient supporté que 80 % des témoignages ne soient pas dans leur langue officielle. Il est très difficile de se concentrer et de tout comprendre quand on écoute l'interprétation. Alors, je vous remercie infiniment. C'était un long passage, alors je voudrais vous remercier.

Ma question s'adresse à vous, monsieur Smith. La Chambre de commerce du Canada a soulevé le fait que le projet de loi C-22 apporte une certaine inquiétude et imprévisibilité, parce qu'elle ne sait pas trop qui va être couvert, à cause de l'absence de définitions, qui seront précisées par voie réglementaire.

Vous semblez partager cette inquiétude. Est-ce que vous pensez que certains secteurs ou fournisseurs devraient être exclus? Je donne les exemples d'Interac ou de Desjardins, dont les représentants nous ont dit qu'ils devraient être exclus. Est-ce que vous pensez qu'on devrait nommer à l'avance des secteurs exclus de la définition de fournisseurs principaux, et qu'on devrait quand même laisser une marge réglementaire au gouvernement, tout en essayant de réduire l'éventail de fournisseurs principaux?

Trouvez-vous que ça pourrait être une solution raisonnable de préciser des fournisseurs principaux, ou de préciser des exclusions, par exemple?

● (1940)

[*Traduction*]

Eric Smith: Merci de la question. Je vais répondre dans ma langue maternelle.

Nous représentons le secteur des télécommunications. Il est bien évident que les entreprises de télécommunications seront considérées comme des fournisseurs principaux. Nous ne nous sommes pas vraiment attardés sur la question de savoir quels autres secteurs seraient classés dans cette catégorie-là et quels autres secteurs dans la catégorie des fournisseurs de services électroniques. Nous savons que ce projet de loi nous vise et c'est vraiment là-dessus que nous nous sommes concentrés.

[*Français*]

Claude DeBellefeuille: Ça va être couvert dans les deux parties. Est-ce que vous vous sentez à l'aise que ce soit dans la partie 1 et dans la partie 2 du projet de loi?

[*Traduction*]

Eric Smith: Le projet de loi lui-même nous préoccupe, mais, pour ce qui est de votre question concernant qui devrait être visé par le projet de loi, nous comprenons que nous serons visés par les parties 1 et 2.

[*Français*]

Claude DeBellefeuille: Monsieur Rankin, vous avez mené les consultations. Si ma mémoire est bonne, vous nous avez dit d'entrée de jeu que vous aviez eu le privilège — je pense qu'on peut le dire ainsi — d'être le premier président de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.

Personnellement, je trouve que cet office, c'est une belle idée. C'est une chance de l'avoir, et je crois beaucoup en son travail. Le gouvernement a choisi de faire des compressions draconiennes à l'Office: il lui a coupé les ailes en diminuant sa capacité à enquêter et à mener des enquêtes d'une manière plus importante. L'Office a subi des coupes de budget de 15 %, soit 2,5 millions de dollars sur un budget de 17 millions de dollars. C'est une réduction assez importante.

Vous avez choisi de ne pas inviter à la table ronde la juge Deschamps, l'actuelle présidente de l'Office. Elle nous a dit qu'elle n'avait pas été invitée à témoigner. Je dois vous dire que, pour moi, ça a été une grande surprise.

Lors de son témoignage devant le Comité, elle a proposé des amendements au projet de loi; au Bloc québécois, nous allons présenter et soutenir ces amendements. Je pense que le gouvernement est bien au courant de notre position sur cette question. La présidente Deschamps nous a dit qu'il serait important, pour elle et pour l'Office, et, surtout, pour rassurer les Canadiens et les Canadiennes, que l'Office soit notifié en temps réel, comme c'est le cas pour le commissaire au renseignement. Ça permettrait de documenter les décisions plutôt que de faire une enquête en utilisant le passé. On a calculé qu'elle serait informée à peu près un an et demi après les interventions. Je trouve que ces amendements sont très raisonnables, surtout que ça ne ralentit aucun processus, parce qu'elle n'a pas accès aux décisions.

Le ministre nous a dit lors de sa comparution que, pour lui, le fait de donner cette capacité alourdirait le processus. Le commissaire au renseignement, soit l'ancien juge Noël, nous a dit que ce n'était pas son opinion, qu'il n'y aurait pas de ralentissement et qu'il était selon lui tout à fait normal qu'elle soit notifiée en temps réel.

Quelle est votre position à cet égard, monsieur Rankin?

L'hon. Murray Rankin: Tout d'abord, je vous remercie de vos commentaires sur mon français. Ça me fait grand plaisir, mais, si vous me le permettez, je vais répondre en anglais à votre question. J'ai passé plusieurs années en Colombie-Britannique, et mon français est un peu rouillé.

[*Traduction*]

Je vais essayer de répondre à votre excellente question dans ma langue maternelle.

Madame la juge Deschamps m'a succédé, et elle fait un excellent travail à l'OSSNR. Je suis au courant des compressions budgétaires, et je partage vos grandes préoccupations à cet égard.

Pour ce qui est du rôle de l'OSSNR, je souligne toutefois que c'est une entité qui effectue des examens après les faits. Actuellement, ce n'est pas un organisme d'examen au sens du projet de loi C-22. Cependant, le commissaire au renseignement doit examiner les arrêtés ministériels. Le commissaire joue déjà le rôle d'examinateur.

Je ne crois pas que l'OSSNR soit bien outillé pour jouer ce genre de rôle. Ce qui serait utile, à mon avis, c'est si on demandait au CPSNR et à l'OSSNR d'effectuer un examen — non pas un examen individuel, comme vous l'envisagez, je crois, mais un examen d'ensemble — du fonctionnement du système, plus tard. Je pense que ce serait très utile.

● (1945)

[*Français*]

Claude DeBellefeuille: Je comprends votre…

Le président: Madame DeBellefeuille, votre temps de parole est malheureusement écoulé.

Monsieur Caputo, vous avez maintenant la parole pour cinq minutes.

[*Traduction*]

Frank Caputo: Merci beaucoup, monsieur le président.

J'aimerais remercier tous les témoins.

Monsieur Milinovich, j'ai écouté attentivement ce que vous avez dit. Ma collègue, Mme Acan, vous a posé une question, et vous avez répondu que cela allait vous prendre beaucoup plus de six minutes, et je comprends pourquoi. Ce n'est pas un dossier facile.

C'est complexe: comment les métadonnées nous aident-elles à retrouver un délinquant, comment une ordonnance de communication est-elle autorisée... Après tout, nous n'avons même pas encore eu le temps d'en parler. Je pense que nous n'avons même pas parlé une fois de ce qu'il faut pour obtenir une ordonnance de communication. Je pense que M. Van Laer nous en a parlé brièvement, la dernière fois, mais nous n'en avons même pas parlé ici. Cela fait partie de ce que j'essaie de faire comprendre. Je sais que mes collègues libéraux pourraient penser que je me répète, mais, en réalité, ce dossier n'est vraiment pas facile. C'est pourquoi nous avons convoqué des avocats, et ils nous ont dit qu'ils n'étaient pas d'accord. C'était des avocats d'expérience, des gens qui pratiquent le droit depuis très longtemps.

J'aimerais vraiment savoir ce que vous en pensez. Je sais que l'extorsion est un problème très important dans votre région. Je crois que nous en avons parlé ensemble pas plus tard que le mois dernier, et j'ai vraiment vu la passion qui vous anime quand vous voulez rendre les rues de la région de Peel plus sécuritaires. Je me fais l'écho de vos propos.

Ce qui ressort de tout cela, selon moi, et cela concerne tous nos témoins ici présents, c'est que nous voulons tous des rues sécuritaires. Nous voulons tous mettre les méchants en prison. Nous voulons tous que les gens qui maltraitent des enfants aillent en prison, et pour très longtemps, c'est moi qui le dis. J'ose espérer que mes collègues libéraux se rangeront derrière nous, or nous voilà en train d'étudier un projet de loi qui a une portée et des répercussions énormes.

Je vais seulement vous poser une petite question, monsieur Rankin. Y a-t-il une recommandation que vous auriez vraiment aimé voir dans le projet de loi, mais qui n'y est pas?

L'hon. Murray Rankin: Pour commencer, merci beaucoup de la question, monsieur Caputo.

Je ne vois pas... Non, je ne peux pas répondre à cette question d'une manière simple. Je ne peux pas.

Frank Caputo: D'accord.

Voici la réalité, monsieur le président. Lorsque M. Powlowski, mon ami et collègue, posait ses questions, il disait qu'il essayait de comprendre les choses. Nous essayons tous de comprendre. C'est la raison pour laquelle j'ai fait référence aux commentaires du chef de police adjoint, M. Milinovich, sur le temps qu'il nous restait.

Une chose que je n'ai cessé de dire, en privé et en public, c'est que nous avons besoin de plus de temps pour ce projet de loi. Certes, nous avons eu trois séances, mais ce n'est certainement pas assez. Ces séances ont été épuisantes. Elles ont duré quatre heures. Nous en sommes à la quatrième heure, et nous ne connaissons toujours pas les choses de base, comme le temps de conservation des métadonnées. Je ne pense pas que nous avons abordé l'aspect technique de la façon dont les métadonnées mènent à une arrestation, à une accusation, qui mène à une condamnation. Nous n'avons même pas abordé le sujet. Nous n'avons pas abordé ce que font le Royaume-Uni, l'Australie, l'Union européenne et la Suède. Nous avons entendu dire que cela prenait 10 mois, un an ou voire deux ans. Nous n'avons pas été plus loin.

Puisque je souhaite voir les méchants derrière les barreaux, je sais que nous devons trouver le juste équilibre et bien faire les choses, tout simplement. Je sais que personne ici présent ne voudrait d'une loi qui, au regard de la Constitution, ne serait pas valide. C'est pour cette raison que je vais présenter une motion. Il me semble que le greffier a reçu des copies en anglais et en français.

Cela ne devrait pas surprendre mes collègues. Je pense que, en tant que conservateurs, nous avons été très transparents sur le sujet. Nous avons été transparents sur la nécessité de tenir plus de réunions.

Monsieur le président, à l'heure actuelle — à l'heure actuelle —, nous devons entendre des témoins jeudi, et pourtant, les amendements doivent être prêts pour demain. En fait, nous allons donc recevoir des représentants officiels alors que le délai pour les amendements sera dépassé.

Je me suis renseigné auprès de M. Rankin. Je pense que nous devrions consacrer une ou deux heures à lui seul. Nous avons lamentablement échoué lorsque nous avons fait comparaître 12 témoins de qualité en une seule réunion, alors que nous aurions pu passer une heure avec chacun d'eux. Nous les avons tous fait comparaître ensemble, et parfois, nous n'avons eu que deux séries de questions.

C'est dans cet esprit que je présente la motion suivante:

> Que, dans le cadre de l'étude en cours du projet de loi C-22, Loi sur l'accès légal,
>
> a) l'étude soit prolongée afin de permettre un examen plus approfondi de la partie 2 du projet de loi, qui vise à promulguer la Loi sur le soutien en matière d'accès autorisé à de l'information, à condition que les témoins suivants comparaissent séparément, pendant au moins une heure chacun:
>
> 1. le ministre de l'Industrie, au sujet des répercussions sur les fournisseurs de services électroniques et leur secteur d'activité,
>
> 2. le ministre responsable du commerce Canada—États-Unis, au sujet des implications en matière de commerce et de sécurité soulevées par les législateurs américains,
>
> 3. le secrétaire d'État (Lutte contre la criminalité),
>
> b) Le comité reçoive 8 heures supplémentaires de témoignages, à condition qu'il donne la priorité à une nouvelle séance d'information avec les responsables ministériels et à l'audition des représentants de Signal, NordVPN, OpenMedia, du Centre pour la liberté d'expression, de la Fondation canadienne pour la Constitution, du Conseil canadien des affaires publiques musulmanes, de l'Association des travailleurs migrants pour le changement, ainsi que les témoignages de Glenn Greenwald, Saffiya Ahmad, Noura Aljizawi, Teresa Scassa et Jane Bailey, en plus de tout autre témoignage jugé pertinent par le comité;
>
> c) Le président soit autorisé à demander du temps de réunion supplémentaire afin de permettre la présentation de ces témoignages en temps opportun,
>
> d) La date limite pour le dépôt des amendements soit reportée jusqu'à ce que les témoignages mentionnés dans la présente motion aient été reçus,
>
> e) Le président ne soit autorisé à fixer une réunion aux fins de l'examen article par article du projet de loi qu'après la comparution des témoins énumérés à la partie a) et la réception du nombre d'heures de témoignage prévu à la partie b).

Monsieur le président, pour les personnes qui ont comparu et qui nous ont parlé de la nécessité de ce projet de loi, pour les victimes et pour les Canadiens, nous devons bien faire les choses, et ce, dès le départ. C'est la raison pour laquelle je présente cette motion.

J'implore mes collègues d'accepter cette motion. Finissons-en avec ce projet de loi. Explorons-le, et faisons bien les choses.

Merci.

● (1950)

[*Français*]

Le président: Merci, monsieur Caputo.

Madame et messieurs les témoins, cela met fin à votre comparution. Nous allons éviter de vous garder avec nous plus longtemps. Étant donné le dépôt de la motion, nous allons certainement passer les prochaines minutes à en discuter. Par conséquent, nous allons éviter de vous priver du plaisir de retourner à la maison ou peu importe où vous souhaitez aller.

[*Traduction*]

J'ai le plaisir de vous annoncer que votre journée touche à sa fin. En revanche, la nôtre n'est pas encore terminée, car nous devons discuter de la motion. Bien évidemment, nous vous sommes très reconnaissants de votre participation, qu'elle soit virtuelle ou en personne. Vos opinions ont été très clairement entendues, mais nous ne les avons pas toutes entendues. Nous espérons pouvoir collaborer davantage avec vous, à l'avenir.

Passez une bonne soirée. Nous n'allons pas suspendre la séance pour vous serrer la main, mais j'imagine que vous comprenez la raison pour laquelle nous devons, à présent, nous concentrer sur notre travail interne. Merci.

[*Français*]

Madame Kirkland, vous avez la parole.

[*Traduction*]

Rhonda Kirkland: Monsieur le président, je crains beaucoup que nous n'ayons pas assez de temps pour bien faire les choses. Quand j'ai parlé aux représentants ministériels, la première fois, avant même que notre comité commence à étudier ce projet de loi, je leur ai dit que ce que nous voulions, pour les personnes qui commettent les crimes les plus haineux, c'est du meilleur régime d'accès légal qui soit, un régime qui puisse faire le travail qu'il est censé faire, et que ce que nous ne voulions pas, c'est d'avoir une chose au détriment d'une autre.

Aujourd'hui, par exemple, notre comité a eu quatre heures. En une heure, nous n'avons eu que deux séries de questions. On a soulevé des questions de privilège, mais ces questions ont été soulevées simplement parce que nous n'avons pas le temps. Nous n'obtenons pas les informations dont nous avons besoin en temps opportun, et ce n'est la faute de personne. C'est parce que le temps ne nous le permet pas.

Nous pouvons toutefois dire que le gouvernement, pour être honnête, a décidé de faire adopter à toute vapeur cette loi et de se dépêcher pour obtenir la sanction royale, comme je l'ai dit à plusieurs reprises. Cela ne rend vraiment pas justice à une loi de cette importance. Les Canadiens méritent de tout entendre. Je sais que j'ai déjà dit que je pouvais poser mes questions aux témoins, en privé, mais ce n'est pas approprié pour les Canadiens. Ils veulent avoir les réponses à ces questions.

Les mots du maire de Brampton m'ont particulièrement choquée et ennuyée. Même si j'ai beaucoup d'estime pour lui, prendre le temps de décortiquer une loi afin de l'étudier, ce n'est pas un signe d'hésitation. C'est notre travail. Si nous ne faisons pas ce travail, à quoi servons-nous ici? D'ailleurs, est-ce également le travail de l'opposition, de se contenter de dire, « oui, oui, oui », de faire le mouton?

Je trouve cela scandaleux que nous ayons prévu si peu de temps. Cela semble approprié de demander huit heures supplémentaires. Cela devrait être facile à faire. Si nous tenons encore des réunions de quatre heures, c'est deux séances de quatre heures supplémentaires.

Je sais que nous sommes fatigués, mais c'est notre travail. Si nous ne faisons pas bien les choses, nous pourrions avoir énormément de problèmes plus tard, et je crains que ce ne soit déjà chose faite. Nous avons vu les nouvelles. Tous ceux qui ont communiqué avec mon bureau ont dit, « effectivement, nous comprenons la nécessité d'un accès légal, mais je me préoccupe de ma vie privée et de ma sécurité. »

J'implore tous les membres du Comité de prendre cette motion au sérieux. Elle a été élaborée de bonne foi. Je veux faire mon travail, et je veux le faire de manière efficace. J'espère que tous les membres du Comité veulent également faire leur travail de manière efficace et examiner avec soin ce projet de loi en faisant bien les choses. C'est vraiment tout ce que nous demandons.

Sur ce, je m'arrête. La seule chose que je tiens à mentionner, c'est le fait que les amendements doivent être prêts avant que nous ayons fini d'entendre les témoignages. Je n'y comprends absolument rien, mais je ne pense pas que ce soit parce que cela fait seulement un an que je suis députée.

● (1955)

Le président: Cela fait peut-être seulement un an que vous êtes ici, mais vous avez l'air d'avoir beaucoup d'expérience.

Je vais donner la parole à M. Ramsay.

Jacques Ramsay: Je remercie M. Caputo et Mme Kirkland d'avoir donné leur avis. Je pense que nous avons une solution qui pourrait plaire à tous, donc nous proposons de reporter le débat.

Rhonda Kirkland: En quoi est-ce une solution?

Frank Caputo: En quoi est-ce une solution?

[*Français*]

Le président: C'est une motion dilatoire sur laquelle nous devons voter immédiatement pour ajourner le débat. Pour être clair, je précise qu'il ne s'agit pas d'ajourner la réunion, il s'agit d'ajourner le débat.

Qui est en faveur de cette motion pour ajourner le débat?

Je crois qu'il est assez clair que la motion est…

[*Traduction*]

Frank Caputo: Nous nous y opposons. Cela devrait être consigné au compte rendu, parce que nous...

Le président: D'accord. Voulez-vous que votre dissidence soit consignée au compte rendu?

Frank Caputo: Non, cela devrait être consigné au compte rendu. Je pense que nous devrions...

Le président: D'accord, si vous voulez, nous pouvons procéder à un vote par appel nominal.

(La motion est adoptée par 6 voix contre 5.)

● (2000)

[*Français*]

Le président: Monsieur Ramsay, la parole est à vous.

Jacques Ramsay: J'aimerais proposer une nouvelle motion:

> Que le comité prolonge son étude du projet de loi C-22 en invitant des témoins à comparaître le jeudi 28 mai, de 16 h 30 à 18 h 30;
>
> Que la date limite pour le dépôt des amendements soit reportée au lundi 1er juin à 17 h 30;
>
> Que la première heure de la réunion du mardi 2 juin soit consacrée au projet de loi C-221, en recevant le parrain du projet de loi…

Claude DeBellefeuille: Excusez-moi de vous interrompre, monsieur Ramsay.

Monsieur le président, est-ce que nous pourrions avoir le texte de la motion sous les yeux?

Le président: Nous allons écouter M. Ramsay, puis nous allons nous assurer que le texte nous est transmis.

Monsieur Ramsay, vous avez la parole.

Jacques Ramsay: Je poursuis:

> Que la première heure de la réunion du mardi 2 juin soit consacrée au projet de loi C-221, en recevant le parrain du projet de loi, Mel Arnold;
>
> Que la deuxième heure de la réunion du mardi 2 juin soit consacrée au témoignage des fonctionnaires concernés sur la question du Budget principal des dépenses ainsi que sur celle du projet de loi C-22;
>
> Et que l'étude article par article du projet de loi C-22 commence le jeudi 4 juin.

Le président: Monsieur Ramsay, avez-vous une version en anglais? Est-ce que vous pouvez la lire en anglais? Comme ça, on va pouvoir l'interpréter en français.

Jacques Ramsay: Oui.

[*Traduction*]

Attendez un instant.

[*Français*]

Claude DeBellefeuille: Monsieur le président, pourquoi n'avons-nous pas le texte de la motion?

Le président: Nous allons voir ce qu'il se passe.

[*Traduction*]

Jacques Ramsay: Alors, le texte se lit comme suit:

> Que le comité prolonge son étude du projet de loi C-22 en invitant des témoins à comparaître le jeudi 28 mai, de 16 h 30 à 18 h 30; Que la date limite pour le dépôt des amendements soit reportée au lundi 1er juin à 17 h 30; Que la première heure de la réunion du mardi 2 juin soit consacrée au projet de loi C-221, en recevant le parrain du projet de loi, Mel Arnold; Que la deuxième heure de la réunion du mardi 2 juin soit consacrée au témoignage des fonctionnaires concernés sur la question du Budget principal des dépenses ainsi que sur celle du projet de loi C-22; Et que l'étude article par article du projet de loi C-22 commence le jeudi 4 juin.

[*Français*]

Le président: Merci.

Nous allons avoir besoin de la transmission de ces informations par courriel, donc par écrit. Le greffier va nous aider à faire ça. Surveillez vos appareils. La motion va être envoyée à la fois en français et en anglais.

Pendant la transmission de l'information, monsieur Caputo, est-ce que vous souhaitez intervenir? Vous êtes inscrit sur ma liste.

[*Traduction*]

Frank Caputo: Avec respect, je vous demanderais de suspendre la séance, pour que je puisse réfléchir à mon intervention une fois que j'aurai lu la motion écrite. J'aimerais voir la motion écrite, s'il vous plaît.

[*Français*]

Le président: Nous allons suspendre la séance, mais je vous dis tout de suite qu'à 20 h 15, nous devons terminer le débat parce que nous n'avons pas les ressources pour continuer au-delà de 20 h 15.

● (2000)

_____(Pause)_____

● (2005)

Le président: Nous reprenons la séance.

Je vous remercie de votre patience. Je crois que tout le monde a reçu la motion proposée par M. Ramsay, dans sa version en français et sa version en anglais.

Monsieur Caputo, vous avez la parole.

● (2010)

[*Traduction*]

Frank Caputo: Merci beaucoup, monsieur le président.

Je remercie M. Ramsay de la motion, même si je pense que notre motion est bien meilleure.

Il faudrait que quelqu'un m'explique le raisonnement ici. Peut-être que je n'ai pas été attentif. Lorsque j'ai d'abord soulevé la question des représentants officiels, selon moi, je l'ai fait de bonne foi. C'est en privé que j'ai dit qu'il y avait quelques problèmes, ici.

Nous avons reçu des représentants pendant une heure, pour parler du projet de loi. Pendant cette heure, ils ont donné très peu de réponses sur les aspects techniques du projet de loi. Je le répète: ce que nous avons entendu jusqu'à présent à propos du projet de loi n'a rien à voir avec les aspects techniques. Cela a à voir avec les aspects philosophiques. Quatre-vingt-dix pour cent de ce que nous avons entendu a à voir avec les aspects philosophiques. Les représentants des forces de l'ordre nous disent eux-mêmes qu'ils en ont vraiment besoin, car cela les aidera à mettre la main au collet des criminels. Eh bien, soit, mais en toute franchise, nous n'avons pas encore abordé les aspects techniques, la mécanique des choses, les choses proprement dites.

J'ai demandé à M. Geist des explications. J'ignore si quelqu'un s'en souvient. Il était ici, et je lui ai demandé ce qu'il en était des métadonnées. Je lui ai demandé ce qu'il en pensait. Il a dit qu'un an, c'était bien trop long. Il a parlé de 30 jours. Je lui ai demandé ce qu'il pensait du fait que, après 30 jours, il n'y aurait peut-être même plus d'enquêteur. M. Van Laer en a parlé. Parfois, vous aurez besoin d'une ordonnance de communication. Parfois, vous ignorez ces choses. Il a dit que, quoi que vous fassiez, il faut que ce soit étayé par des preuves. C'était sa réponse.

Pouvons-nous dire que, aujourd'hui, nous avons pu établir un délai? Nous avons entendu parler ce qui se passe ailleurs dans le monde — en Suède, apparemment, c'est 10 mois, et en Australie, apparemment, c'est deux ans — et des choses de ce genre. C'est pour cette raison précise que je pense que les représentants sont si essentiels. Nous n'avons pas encore abordé les aspects techniques, donc, nous avons beau en parler, je pense quand même que nous devons entendre beaucoup plus de témoins.

Je vais simplement regarder la motion, ici. La date limite pour le dépôt des amendements est lundi, à 17 h 30. Certes, le jeudi 28, nous recevons des témoins, mais le problème reste entier: la date limite de dépôt des amendements est lundi, nous recevons des représentants mardi et nous passons à l'étude article par article jeudi. Pourquoi recevons-nous des représentants après la date limite de dépôt des amendements?

C'est une question de pure forme. Je ne m'attends pas à une réponse. Je pense que, de toute façon, je n'aurais pas de réponse.

J'ai l'impression que M. Powlowski a vraiment hâte de me donner une réponse. Il vient à peine de comprendre le projet de loi, cela lui a pris les 45 dernières minutes, ou quelque chose comme ça.

Je ne prends pas cela à la légère. Je le crois lorsqu'il dit « nous n'y comprenons vraiment rien. »

D'accord, Mme Acan comprend vraiment le projet de loi.

Sima Acan: Il n'a pas dit « nous ».

Effectivement, je l'ai compris.

Frank Caputo: J'essaie toujours de comprendre le contenu de ce projet de loi. Par conséquent, afin de respecter notre obligation en tant que loyale opposition de Sa Majesté, nous devrions avoir le droit d'entendre le témoignage complet des représentants avant de présenter nos amendements. Sinon, nous allons essentiellement procéder à une étude article par article glorifiée, car, dans ce cas, nous allons faire comparaître des représentants après avoir présenté nos amendements, ce que, de toute façon, nous ferions normalement dans le cadre d'une étude article par article. C'est un peu comme si nous repoussions l'inévitable. Nous ne suivons pas vraiment un processus approprié.

Je réitère que ce projet de loi a fait l'objet d'une contestation considérable, et, si je peux me permettre, de l'opposition considérable de certaines personnes. Aujourd'hui, on a dit que de nombreuses personnes étaient en faveur de ce projet de loi. Il y a un groupe qui est assez favorable à ce projet de loi. Un autre groupe est plutôt opposé à ce projet de loi. Notre travail est d'essayer de trouver un juste équilibre où, d'un côté, les criminels sont placés derrière les barreaux, et de l'autre, la vie privée et les droits prévus par la Charte sont protégés. Je pense que tous les gens ici présents souhaiteraient cela. Mais comment faire, lorsque la date limite du dépôt des amendements précède la date de comparution des représentants? En ce qui me concerne, il est parfaitement raisonnable de faire comparaître des représentants avant de présenter des amendements. Je ne comprends pas pourquoi nous ne le ferions pas.

Par exemple, prenons la partie 1, et comparons « motifs raisonnables soupçonnés » à « motifs raisonnables de croire ». Nous avons entendu le commissaire Carrique parler du seuil inférieur. La seule fois où nous avons vraiment parlé des motifs raisonnables de soupçonner par rapport aux motifs raisonnables de croire, c'est lorsque j'ai posé la question.

Si je me souviens bien, on parle de motifs raisonnables de croire quand un agent de la paix croit — et non pas soupçonne — personnellement ou subjectivement qu'une infraction a été commise et que ce qu'il croit est raisonnablement objectif. C'est la définition des motifs raisonnables de croire, ou du moins, c'était la définition il y a cinq ans lorsque je pratiquais toujours le droit.

● (2015)

Anthony Housefather: Pour information, monsieur le président.

Le président: Une question d'information n'est pas vraiment un rappel au Règlement, mais...

Anthony Housefather: J'aimerais savoir jusqu'à quand nous aurons des ressources pour la réunion...

Le président: Voilà une excellente question.

Anthony Housefather: ... car si nous continuons, la date limite de dépôt des amendements sera demain, et nous amorcerons l'étude article par article mardi. J'essaie de savoir à quelle heure nous devons arrêter.

Le président: C'est un rappel au Règlement sous forme de question d'information.

Je ne suis pas avocat, donc vous pourriez le décrire mieux que moi, mais c'est un commentaire très juste, et j'allais le faire.

Il ne nous reste que trois minutes avant la levée de séance.

Comme M. Housefather l'a dit, si nous ne votons pas sur cette motion-là, nous avons la motion existante, qui l'emporte. Cela signifie que nous allons procéder à l'étude article par article mardi prochain — le 2 juin —, et que la date limite de dépôt des amendements est demain. Je vous le ferai savoir, car nous avons une motion par défaut, un ordre du jour par défaut, que nous avons adopté. Nous avons à présent l'occasion de voter sur un différent ordre du jour. Nous devons maintenant avoir terminé cela dans deux minutes.

Sommes-nous prêts à procéder au vote?

Frank Caputo: J'ai toujours la parole, monsieur le président...

Le président: Oui, monsieur Caputo.

Frank Caputo: ... à moins que Mme Kirkland ne veuille vraiment avoir la parole.

Rhonda Kirkland: Effectivement.

Le président: Vous avez deux minutes, madame Kirkland.

Rhonda Kirkland: J'ai une question. Qu'est-ce qu'il y a jeudi? Qu'allons-nous faire à la prochaine réunion?

Le président: Jeudi, nous recevons le ministre pour une heure, pour parler du budget principal des dépenses, et nous avons deux heures pour... Nous allons consacrer une heure au ministre et une heure aux représentants, et ensuite, nous consacrons une heure supplémentaire aux représentants pour l'étude du projet de loi C-22. Les trois heures de jeudi seront consacrées, pour la première, au ministre, pour la deuxième, aux représentants, sur le budget principal des dépenses, et pour la dernière, au projet de loi C-22.

Rhonda Kirkland: Effectivement, je souhaite poser une question, mais je ne veux pas céder la parole pour autant. C'est ce qui me préoccupe.

Je ne vois vraiment pas en quoi ce serait une solution. Je sais ce que M. Ramsay a dit: « Oh, j'ai une solution: ajournons le débat sur votre motion et permettez-moi de présenter cette magnifique motion, qui est la solution à tous nos problèmes. »

La solution semble être de conserver le même scénario, selon lequel nous devons déposer les amendements avant d'avoir reçu tous les représentants ministériels et prévoir deux heures supplémentaires pour entendre les témoins. En toute franchise, nous avons reçu 18 témoins, ici, aujourd'hui. Je sais que M. Caputo a dit que nous en avons reçu 12. Nous avons eu 18 témoins ici, aujourd'hui: 18 personnes et peut-être 12 ou 13 organisations. Nous n'avons pas pu leur poser de questions.

Ce qui me préoccupe, c'est que nous n'avons pas eu assez de temps. Nous n'avons pas du tout le temps. En toute franchise, je pense que le gouvernement abuse de son pouvoir en faisant adopter le projet de loi à toute vapeur, sans donner à l'opposition l'occasion d'interroger adéquatement les témoins, de façon à ce que nous puissions adopter un projet de loi bien fait. Nous voulons un projet de loi bien fait. Nous le voulons.

Je suis un peu choquée. En réalité, je suis vraiment choquée de constater que nous ne voulons pas faire notre travail, que nous ne voulons pas consacrer trop de temps à ce projet de loi, et que nous voulons simplement foncer tête baissée, au détriment des Canadiens, de leur vie privée et de leurs droits. Pour être honnête, je suis perplexe de voir que personne, ici, n'y voit d'inconvénient. Je suis très perplexe. Je ne comprends absolument pas.

Lorsque j'ai commencé à entendre parler de ce projet de loi, et lorsque je l'ai examiné...

● (2020)

Le président: Je vais devoir vous interrompre très bientôt.

Rhonda Kirkland: D'accord. C'est donc ici que je m'arrête.

Vous m'interrompez pour conclure la séance? C'est bien cela?

Le président: Oui, car nous n'avons plus de ressources, c'est-à-dire que les interprètes et les techniciens doivent partir.

Rhonda Kirkland: D'accord, je...

Le président: Permettez-moi de donner une autre information. Je peux lever la séance, mais cela signifie que nous n'allons pas recevoir le ministre jeudi. Le ministre est censé comparaître au sujet du budget principal des dépenses, jeudi. Si je suspends la discussion, ce qui est possible, cela signifie que nous n'allons pas recevoir le ministre, jeudi.

Normalement, je lève la séance, ce que je ferai dans une seconde. Cela veut dire que nous allons suivre la motion existante établissant l'ordre du jour, à moins que, au cours des quelques prochaines heures, on décide de la modifier, dans le cadre de discussions à l'extérieur de cette séance.

Je lève donc la séance et je vous souhaite à tous une bonne soirée.