EVIDENCE

OTTAWA, Monday, November 2, 2026

The Standing Senate Committee on National Security, Defence and Veterans Affairs met this day at 4:01 p.m. [ET] to study Bill C-22, An Act respecting lawful access; and to study Bill S-223, An Act to amend the Royal Canadian Mounted Police Act; and, in camera, to examine and report on defence procurement in the context of Canada's commitment to increase defence spending.

Senator Marty Deacon (*Chair*) in the chair.

[*English*]

The Chair: I'd like to extend a big welcome to everybody. I'm Marty Deacon, senator from Ontario, and chair of the committee. We have a full house, we have a full evening and we have a bill that we are launching this evening, so I want to take an opportunity to thank not only the people at the table but also the support teams around the table, behind the table and, probably, in the hallway. I thank you very much for all of you being here this evening.

I would like to begin today by offering my colleagues the opportunity to introduce themselves.

Senator Dhillon: Good afternoon. Baltej Dhillon, B.C.

[*Translation*]

Senator Dalphond: Good afternoon. Pierre Dalphond, Quebec.

[*English*]

Senator Patterson: Rebecca Patterson, Ontario.

Senator Ross: Krista Ross, New Brunswick.

Senator Pate: Good afternoon and welcome. Kim Pate. I live here on the unceded, unsurrendered and unreturned territory of the Algonquin Anishinaabeg.

Senator Dean: Tony Dean, Ontario.

Senator Cardozo: Andrew Cardozo.

Senator Tucker: Geeta Tucker, Manitoba.

[*Translation*]

Senator Martel: Good afternoon to you all. Richard Martel, Quebec.

TÉMOIGNAGES

OTTAWA, lundi 2 novembre 2026.

Le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants se réunit aujourd'hui, à 16 h 01 (HE) pour étudier le projet de loi C-22, Loi concernant l'accès légal; pour étudier le projet de loi S-223, Loi modifiant la Loi sur la Gendarmerie royale du Canada, et, à huis clos, pour examiner, afin d'en faire rapport, l'approvisionnement en matière de défense dans le contexte de l'engagement du Canada à accroître ses dépenses de défense.

La sénatrice Marty Deacon (*présidente*) occupe le fauteuil.

[*Traduction*]

La présidente : J'aimerais souhaiter la bienvenue à tout le monde. Je m'appelle Marty Deacon, sénatrice de l'Ontario et présidente du comité. La salle est comble, la soirée s'annonce bien remplie et nous avons un projet de loi à présenter ce soir. Je tiens donc à profiter de l'occasion pour remercier non seulement les personnes assises à la table, mais aussi les équipes de soutien autour de la table, derrière la table et, probablement, dans le couloir. Je vous remercie tous sincèrement d'être ici ce soir.

J'aimerais commencer aujourd'hui en donnant à mes collègues l'occasion de se présenter.

Le sénateur Dhillon : Bonjour. Baltej Dhillon, de la Colombie-Britannique.

[*Français*]

Le sénateur Dalphond : Bonjour. Pierre Dalphond, du Québec.

[*Traduction*]

La sénatrice Patterson : Rebecca Patterson, de l'Ontario.

La sénatrice Ross : Krista Ross, du Nouveau-Brunswick.

La sénatrice Pate : Bonjour et bienvenue. Kim Pate. Je vis ici, sur le territoire non cédé, non abandonné et non restitué du peuple algonquin anishinabe.

Le sénateur Dean : Tony Dean, de l'Ontario.

Le sénateur Cardozo : Andrew Cardozo.

La sénatrice Tucker : Geeta Tucker, du Manitoba.

[*Français*]

Le sénateur Martel : Bonjour à vous tous. Richard Martel, du Québec.

[*English*]

Senator McNair: Welcome. John McNair, New Brunswick.

Senator Hay: Katherine Hay, Ontario.

The Chair: Today, we begin our examination of Bill C-22, An Act respecting lawful access. We will hear from three panels of witnesses.

For the first panel this evening, we are pleased to welcome from the Office of the Privacy Commissioner of Canada, Philippe Dufresne, Privacy Commissioner of Canada; and Marc Chénier, Deputy Commissioner and Senior General Counsel. We also have, from the National Security and Intelligence Review Agency, Craig Forcese, Vice-Chair; and Lawrence Mangano, Acting Executive Director (Chief Executive and Deputy Head). Finally, from the Office of the Intelligence Commissioner, the Honourable Simon Noël, K.C., Intelligence Commissioner; and Justin Dubois, Executive Director and General Counsel.

It's a full slate. Welcome to all of our guests. We will begin by inviting you to provide opening remarks, to be followed by questions from our members. We will begin with Mr. Dufresne.

[*Translation*]

Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada: Thank you, Madam Chair, honourable members of the committee, for the invitation to share my views on Bill C-22, An Act respecting lawful access.

Canadian law enforcement, security and intelligence agencies are facing new challenges arising from technological developments, the varying interception capabilities of service providers, and jurisdictional issues stemming from the cross-border nature of digital crime. Bill C-22 is specifically designed to address some of these challenges, including by requiring electronic service providers to provide reasonable assistance to state authorities in the exercise of their statutory powers.

[*English*]

The policy objectives of Bill C-22 are important, and the current bill incorporates significant improvements over previous versions, including a number of welcome changes adopted by the other place. For example, an amendment to Part 1 enhances judicial oversight by clarifying that a justice or judge may specify the information that must be produced under the new production order for subscriber information. Amendments to Part

[*Traduction*]

Le sénateur McNair : Bienvenue. John McNair, du Nouveau-Brunswick.

La sénatrice Hay : Katherine Hay, de l'Ontario.

La présidente : Aujourd'hui, nous entamons notre examen du projet de loi C-22, Loi sur l'accès légal. Nous entendrons trois groupes de témoins.

Pour le premier groupe de ce soir, nous sommes heureux d'accueillir Philippe Dufresne, commissaire à la protection de la vie privée du Canada, et Marc Chénier, sous-commissaire et avocat général principal, du Commissariat à la protection de la vie privée du Canada. Nous accueillons également Craig Forcese, vice-président, et Lawrence Mangano, directeur général par intérim, directeur général et directeur adjoint, de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. Enfin, nous accueillons l'honorable Simon Noël, c.r., commissaire au renseignement, et Justin Dubois, directeur exécutif et avocat général, du Bureau du commissaire au renseignement.

C'est un programme bien rempli. Bienvenue à tous nos témoins. Nous allons commencer par vous inviter à présenter des observations préliminaires, puis nous passerons aux questions des membres du comité. Nous commencerons par M. Dufresne.

[*Français*]

Me Philippe Dufresne, commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada : Merci, madame la présidente, mesdames et messieurs membres du comité, pour cette invitation à exprimer mon point de vue sur le projet de loi C-22, la Loi concernant l'accès légal.

Les organismes canadiens d'application de la loi, de sécurité et de renseignement sont confrontés à de nouveaux défis en raison des progrès technologiques, des capacités d'interception variables d'un fournisseur de services à l'autre et des questions de compétence liées à la nature transfrontalière de la criminalité numérique. Le projet de loi C-22 est expressément conçu pour faire face à certains de ces défis, notamment en obligeant les fournisseurs de services électroniques à offrir une aide raisonnable aux acteurs étatiques dans l'exercice de leurs pouvoirs prévus par la loi.

[*Traduction*]

Les objectifs stratégiques du projet de loi C-22 sont importants, et le projet de loi actuel comporte des améliorations importantes aux versions précédentes, y compris plusieurs modifications bienvenues adoptées par l'autre Chambre. Par exemple, un amendement à la partie 1 renforce la surveillance judiciaire en expliquant qu'un juge peut préciser les renseignements qui doivent être communiqués en vertu de la

2 preclude requirements to decrypt end-to-end encrypted information, impose new limits on the proposed regulatory information and order-making powers, and allow for appropriate disclosures to regulatory authorities.

[*Translation*]

These are positive measures. However, despite these improvements, further amendments would be needed to better protect the privacy of Canadians while continuing to provide state authorities with the tools they need to carry out their important work.

First, in the amended version of the bill, the proposed definition of "subscriber information" and the range of persons from whom such information could be obtained under the new production order remain broad relative to the reasonable suspicion threshold required to access it.

[*English*]

Depending on the nature of the service providers in question, which include health care providers, lawyers, financial institutions and dating apps, such information could reasonably attract a heightened expectation of privacy due to its sensitivity. For this reason, I would recommend narrowing the definition of "subscriber information" to a finite list of discrete identifiers and restricting the range of persons or entities from whom it may be compelled to telecommunication service providers. In the alternative, I would recommend adding a carve-out for medical or privileged information to the new production order, as is the case under the proposed confirmation of service demand.

Second, the bill would clarify that police do not require a production order or warrant for any information that is available to the public. However, the concept of publicly available information is undefined, and an individual does not automatically forfeit any reasonable expectation of privacy in information that has become public. I would, therefore, recommend defining "publicly available information" in such a way as to exclude information in respect of which a person has a reasonable expectation of privacy, consistent with the definition in the Communications Security Establishment Act.

nouvelle ordonnance de communication des renseignements relatifs à l'abonné. Les amendements à la partie 2 excluent l'obligation de décrypter les renseignements chiffrés de bout en bout, imposent de nouvelles limites aux pouvoirs réglementaires proposés en matière de renseignements et de prise d'ordonnances, et permettent la communication appropriée de renseignements aux autorités réglementaires.

[*Français*]

Ces mesures sont positives. Toutefois, malgré ces améliorations, des amendements supplémentaires seraient nécessaires afin de mieux protéger la vie privée des Canadiennes et des Canadiens tout en continuant à fournir aux autorités étatiques les outils nécessaires pour accomplir leur travail important.

Premièrement, dans la version modifiée du projet de loi, la définition proposée du terme « renseignements relatifs à l'abonné » et l'éventail des personnes auprès desquelles ces renseignements pourraient être obtenus au titre de la nouvelle ordonnance de communication demeurent larges par rapport aux critères de soupçon raisonnable requis pour y avoir accès.

[*Traduction*]

Selon la nature des fournisseurs de services en question, qui comprennent les prestataires de soins de santé, les avocats, les institutions financières et les applications de rencontre, ces renseignements pourraient vraisemblablement donner lieu à une attente accrue en matière de protection de la vie privée en raison de leur caractère sensible. C'est pourquoi je recommande de restreindre la définition des « renseignements relatifs à l'abonné » à une liste limitée d'identifiants distincts et de limiter l'éventail des personnes ou entités auprès desquelles ces renseignements peuvent être exigés aux fournisseurs de services de télécommunications. À titre subsidiaire, je recommande d'ajouter à la nouvelle ordonnance de communication une exception pour les renseignements médicaux ou protégés par le secret professionnel, comme c'est le cas dans les ordres de confirmer la fourniture de services proposés.

Deuxièmement, le projet de loi précise que la police n'a pas besoin d'une ordonnance de communication ni d'un mandat pour obtenir des renseignements accessibles au public. Cependant, la notion de renseignements accessibles au public n'est pas définie, et une personne ne renonce pas automatiquement à toute attente raisonnable en matière de protection de la vie privée en ce qui concerne des renseignements devenus publics. Je recommande donc de définir les « renseignements accessibles 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.

[*Translation*]

Third, although the House amended Part 1 to provide that a judge may specify the information to be disclosed pursuant to the new subscriber information production order, it did not update the relevant prescribed forms that must be used to obtain such orders. I recommend that this apparent oversight be corrected in order to avoid any inconsistency between the forms and the applicable legal requirements.

[*English*]

Fourth, while the bill provides that both the Governor-in-Council and the Minister of Public Safety would have to consider several factors when making regulations or orders, including their potential impacts on privacy protection and cybersecurity, there's no overarching requirement that all obligations imposed under the act be both necessary and proportionate. As it is a key privacy principle in Canada and around the world, I would recommend that necessity and proportionality be made requirements under the act.

Fifth and last, given the debates and the stakeholder and industry concerns with respect to the need to avoid creating systemic vulnerabilities, I would recommend amending the bill's compliance enforcement framework to allow electronic service providers to trigger a pre-emptive arm's-length assessment by qualified experts, as in comparable laws in the United Kingdom, Australia and New Zealand.

Taken together, I believe that these changes would help ensure the appropriate balance between law enforcement, national security and Canadians' fundamental right to privacy.

Thank you, and I look forward to your questions.

The Chair: Thank you very much.

[*Translation*]

The Honourable Simon Noël, K.C., Intelligence Commissioner: Thank you, Madam Chair and honourable members of the committee, for the opportunity to discuss Bill C-22 with you. I am accompanied by Justin Dubois, my office's Executive Director and General Counsel.

As Intelligence Commissioner, or IC, I fulfill an independent quasi-judicial oversight role. I approve, or do not approve, ministerial decisions authorizing certain national security and intelligence activities proposed by the Communications Security Establishment Canada and the Canadian Security Intelligence Service. I assess whether the minister's justification for allowing

[*Français*]

Troisièmement, bien que la Chambre ait modifié la partie 1 afin d'indiquer qu'un juge peut préciser les renseignements qui doivent être communiqués conformément à la nouvelle ordonnance de communication des renseignements relatifs à l'abonné, elle n'a pas mis à jour les modèles de formulaires pertinents qui doivent être utilisés pour obtenir de telles ordonnances. Je recommande de corriger cette omission apparente afin d'éviter toute incohérence entre les formulaires et les obligations juridiques applicables.

[*Traduction*]

Quatrièmement, bien que le projet de loi prévoie que le gouverneur en conseil et le ministre de la Sécurité publique doivent tenir compte de plusieurs facteurs lorsqu'ils adoptent des règlements ou qu'ils rendent des ordonnances, y compris de leurs répercussions potentielles sur la protection de la vie privée et la cybersécurité, il n'existe aucune exigence générale selon laquelle toutes les obligations imposées en vertu de la loi doivent être à la fois nécessaires et proportionnées. Comme il s'agit d'un principe clé de protection de la vie privée au Canada et partout dans le monde, je recommande que la nécessité et la proportionnalité soient érigées en exigences en vertu de la loi.

Cinquièmement et enfin, compte tenu des débats et des préoccupations des intervenants et de l'industrie quant à la nécessité d'éviter de créer des vulnérabilités systémiques, je recommande de modifier le cadre d'application de la conformité du projet de loi afin de permettre aux fournisseurs de services électroniques de déclencher une évaluation préventive indépendante menée par des experts qualifiés, comme c'est le cas dans des lois comparables en vigueur au Royaume-Uni, en Australie et en Nouvelle-Zélande.

Je crois qu'ensemble, ces modifications aideraient à trouver un juste équilibre entre l'application de la loi, la sécurité nationale et le droit fondamental des Canadiens à la vie privée.

Merci. Je serai heureux de répondre à vos questions.

La présidente : Merci beaucoup.

[*Français*]

L'honorable Simon Noël, c.r., commissaire au renseignement : Madame la présidente, honorables membres du comité, je vous remercie de votre invitation à discuter du projet de loi C-22. Je suis accompagné de Me Justin Dubois, directeur exécutif et avocat général de mon bureau.

Comme commissaire au renseignement, j'exerce un rôle de surveillance indépendant et quasi judiciaire. J'approuve ou je n'approuve pas les décisions ministérielles autorisant certaines activités de sécurité nationale et de renseignement proposées par le Centre de la sécurité des télécommunications Canada et le Service canadien du renseignement de sécurité. J'évalue si la

these activities is reasonable, which includes compliance with the Charter.

Part 2 of Bill C-22 would give the IC a new responsibility to review decisions of the Minister of Public Safety to issue orders to electronic service providers.

[*English*]

This new responsibility resembles my current work. I already review ministerial decisions that are not made public. For each ministerial decision, the legislation sets out what the minister must consider. The privacy of Canadians is a central concern, as it would be under Bill C-22.

I would apply the same principles of administrative law applied by Canadian courts. My decision would be shared with NSIRA, published with appropriate redactions and subject to judicial review by the Federal Court.

There would be new elements, nevertheless. An electronic service provider would have an opportunity to make representations to the minister, which would form part of the record before me. Also, the Intelligence Commissioner's decision would concern obligations imposed upon the private sector service provider rather than activities conducted by CSIS or CSE.

I welcome the House amendments responding to some of the issues I raised. Orders are now limited to two years. It is also now clear that the minister must consider the listed factors in deciding whether to make an order.

I would raise an additional issue the committee might wish to consider; it is the same one raised by the Privacy Commissioner: Should the bill explicitly require the minister to consider proportionality as a factor when deciding whether to make an order? Subclause 7(3) of Part 2 states only that the minister must take into account the factors, but it does not explicitly require the minister to explain why the balance of the factors favours making the confidential order or to consider reasonable alternatives. It is also not clear that the minister must consider whether it is justified to proceed by ministerial order and, therefore, by a confidential process.

justification du ministre pour autoriser ces activités est raisonnable, ce qui comprend la conformité à la Charte.

La partie 2 du projet de loi C-22 confierait au commissaire une nouvelle responsabilité, soit d'examiner les décisions du ministre de la Sécurité publique et de prendre des arrêtés visant des fournisseurs de services électroniques.

[*Traduction*]

Cette nouvelle responsabilité ressemble à mon travail actuel. J'examine déjà les décisions ministérielles qui ne sont pas rendues publiques. Pour chaque décision ministérielle, la loi énonce les éléments que le ministre doit prendre en considération. La protection de la vie privée des Canadiens est une préoccupation centrale, comme ce serait le cas en vertu du projet de loi C-22.

J'appliquerai les mêmes principes de droit administratif que ceux appliqués par les tribunaux canadiens. Ma décision sera communiquée à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, publiée après les expurgations appropriées et soumise au contrôle judiciaire de la Cour fédérale.

Il y a néanmoins de nouveaux éléments. Un fournisseur de services électroniques aura la possibilité de présenter des observations au ministre, lesquelles seront versées au dossier qui me sera soumis. De plus, la décision du commissaire au renseignement portera sur les obligations imposées au fournisseur de services du secteur privé, au lieu des activités menées par le Service canadien du renseignement de sécurité, le SCRS, ou le Centre canadien pour la cybersécurité, le CST.

Je salue les modifications apportées par la Chambre qui répondent à certaines des questions que j'ai soulevées. Les ordonnances sont maintenant limitées à deux ans. Il est également clair à présent que le ministre doit tenir compte des facteurs énumérés avant de décider s'il y a lieu de rendre une ordonnance.

Je voudrais poser une autre question que le comité pourrait souhaiter examiner. C'est la même que celle posée par le commissaire à la protection de la vie privée : le projet de loi devrait-il prévoir explicitement que le ministre tienne compte de la proportionnalité comme facteur lorsqu'il décide de rendre ou non une ordonnance? Le paragraphe 7(3) de la partie 2 stipule seulement que le ministre doit tenir compte des facteurs, mais il ne prévoit pas explicitement que le ministre explique pourquoi, au regard de l'ensemble des facteurs en jeu, il est préférable de rendre une ordonnance confidentielle ou d'envisager d'autres solutions raisonnables. Il n'est pas non plus clair que le ministre doive se demander s'il est justifié de procéder par arrêté ministériel et, par conséquent, dans le cadre d'un processus confidentiel.

Nothing prevents the minister from addressing these questions, but the bill does not clearly require their consideration. If the intent of ministerial orders is to respond to situations where confidentiality is necessary, a clear proportionality factor that includes reasonable alternatives would ensure that the minister explains the needs.

[*Translation*]

This matters because my review is limited to the conclusions the minister makes pursuant to subclause 7(3). As the Supreme Court of Canada made clear in *Vavilov*, I must assess the decision the minister actually made and the reasons actually given. Making it explicit in the bill that the minister must address proportionality would guarantee this factor is included in my review.

Finally, as I've already stated, if additional resources are required for me to fulfill my mandate, I expect they will be provided.

I would be pleased to answer any questions that may be of particular interest to committee members.

Thank you, chair.

[*English*]

The Chair: Thank you very much, Mr. Noël. We appreciate that.

[*Translation*]

Craig Forcese, Vice-Chair, National Security and Intelligence Review Agency: Madam Chair, members of the committee, good afternoon.

Thank you for your invitation to appear today.

[*English*]

I will address four points today: first, NSIRA's role in the lawful access activities currently under consideration; second, the continued importance of timely access to relevant information; third, the reality NSIRA currently faces; and fourth, the way forward.

[*Translation*]

First, let's talk about NSIRA's role. The provisions in this bill will require notification to NSIRA about the use of the new lawful access powers. The agency's work helps to ensure that national security and intelligence powers are exercised lawfully, reasonably and only when necessary.

Rien n'empêche le ministre de traiter ces questions, mais le projet de loi ne prévoit pas clairement qu'il en tienne compte. Si l'intention des arrêtés ministériels est de répondre à des situations où la confidentialité est nécessaire, un facteur de proportionnalité clair, incluant des solutions de rechange raisonnables, garantirait que le ministre explique les besoins.

[*Français*]

Cela est important, parce que mon examen se limite aux conclusions que le ministre tire au titre du paragraphe 7(3). Comme établi par la Cour suprême du Canada dans l'arrêt *Vavilov*, je dois évaluer la décision que le ministre a rendue et les motifs qu'il a donnés. Prévoir expressément dans le projet de loi que le ministre doit se pencher sur la proportionnalité garantirait que ce facteur fasse partie de mon examen.

Enfin, comme je l'ai déjà mentionné, si des ressources supplémentaires s'avèrent nécessaires pour m'acquitter de mon mandat, je m'attends à ce qu'elles soient fournies.

Je serai heureux de répondre à vos questions qui pourraient être d'intérêt pour chacun et chacune d'entre vous.

Merci, madame.

[*Traduction*]

La présidente : Je vous remercie, monsieur Noël. Nous vous savons gré de vos observations.

[*Français*]

Craig Forcese, vice-président, Office de surveillance des activités en matière de sécurité nationale et de renseignement : Madame la présidente, membres du comité, bonjour.

Je vous remercie de votre invitation à comparaître devant vous aujourd'hui.

[*Traduction*]

Je parlerai de quatre points aujourd'hui : premièrement, le rôle de l'OSSNR dans les activités d'accès légal actuellement à l'étude; deuxièmement, l'importance constante d'un accès en temps opportun à l'information pertinente; troisièmement, la réalité à laquelle l'OSSNR fait face actuellement; et quatrièmement, la voie à suivre.

[*Français*]

Parlons d'abord du rôle de l'OSSNR. Les dispositions prévues dans ce projet de loi obligeraient les institutions concernées à aviser l'office du recours aux nouveaux pouvoirs d'accès légal. L'office contribue à faire en sorte que les pouvoirs en sécurité nationale et des renseignements soient exercés légalement, de façon raisonnable et uniquement lorsque cela est nécessaire.

[*English*]

We have the power to pick most of our review topics based upon careful consideration of criteria that we have published online. Consequently, the government does not choose what we do or do not review. Therefore, NSIRA's role, should Bill C-22 be enacted, will be significant and vital.

Second is the importance of timely access to information. The lifeblood of NSIRA's review work is timely access to information to which we have a legal right. We look forward to this timely access under the proposed notification regime, should Bill C-22 be enacted.

[*Translation*]

Third is NSIRA's reality.

As new authorities expand the scope and complexity of national security and intelligence activities, our purview also expands. Our resources have not kept pace. Indeed, the opposite has been true. As a result, NSIRA has had to make and will continue to confront difficult decisions about how best to prioritize and deploy its resources.

[*English*]

Fourth is the way forward. Last week, the government released its national security strategy, in which it committed to reviewing the entire national security enterprise, including review and oversight bodies.

[*Translation*]

After more than seven years in operation, NSIRA has established a strong record of independent review. Drawing on that experience, NSIRA has provided proposals to government regarding potential legislative amendments to the NSIRA act that would strengthen and modernize the review framework.

[*English*]

These proposals are informed by lessons learned through our reviews and public complaint investigations. They are intended to improve the effectiveness, efficiency and long-term sustainability of independent review. They aim to ensure that review mechanisms keep pace with evolving authorities, like those in Bill C-22; emerging technologies; and an increasingly complex operating environment.

[*Traduction*]

Nous avons la possibilité de choisir la plupart de nos sujets d'examen en nous fondant sur une analyse minutieuse des critères que nous avons publiés en ligne. Ce n'est donc pas le gouvernement qui décide de ce que nous examinons ou pas. Par conséquent, si le projet de loi C-22 est adopté, le rôle de l'OSSNR sera important et essentiel.

Deuxièmement, l'importance d'un accès à l'information en temps opportun. Il est vital pour le travail d'examen de l'OSSNR d'avoir accès rapidement à l'information à laquelle il a légalement droit. Nous nous réjouissons de pouvoir bénéficier de cet accès en temps opportun dans le cadre du régime de notification proposé, si le projet de loi C-22 vient à être adopté.

[*Français*]

Examinons maintenant la réalité à laquelle l'office est confronté.

À mesure que de nouveaux pouvoirs élargissent la portée et la complexité des activités en matière de sécurité nationale et de renseignement, le champ de compétence de l'office s'élargit lui aussi. Nos ressources, toutefois, n'ont pas suivi cette évolution. En fait, c'est plutôt le contraire. Par conséquent, l'office a dû prendre, et continuera de devoir prendre, des décisions difficiles quant à la meilleure façon de prioriser ses travaux.

[*Traduction*]

Quatrièmement, la voie à suivre. La semaine dernière, le gouvernement a publié sa stratégie en matière de sécurité nationale, dans laquelle il s'engage à revoir l'ensemble de l'organisation de la sécurité nationale, y compris les organismes d'examen et de surveillance.

[*Français*]

Après plus de sept années d'existence, l'office a établi un solide bilan en matière d'examen indépendant. Fort de cette expérience, l'office a soumis au gouvernement des propositions de modifications législatives afin de renforcer et de moderniser le cadre d'examen.

[*Traduction*]

Ces propositions s'appuient sur les leçons tirées de nos examens et de nos enquêtes sur les plaintes du public. Elles visent à améliorer l'efficacité, l'efficience et la viabilité à long terme de l'examen indépendant. Elles visent à garantir que les mécanismes d'examen suivent l'évolution des pouvoirs, comme ceux prévus dans le projet de loi C-22, des technologies émergentes et d'un environnement opérationnel de plus en plus complexe.

[*Translation*]

As the government considers broader reforms to Canada's review and oversight framework, NSIRA stands ready to contribute its expertise.

[*English*]

To conclude, the notification provisions in this bill, when paired with timely access to relevant information and NSIRA's independent discretion to prioritize its reviews, will assist our ability to evaluate the use of these powers.

[*Translation*]

Our independent review helps ensure that powers are exercised responsibly, risks are appropriately managed, and Canada's national security institutions remain worthy of the trust placed in them by Canadians.

[*English*]

Meeting these objectives will depend upon proper funding and updated legislation. It will also continue to require a government culture that is responsive to the essential role of robust review in guarding faith in the necessary activities of intelligence and security agencies.

[*Translation*]

Thank you for your attention. We would be pleased to answer your questions.

[*English*]

The Chair: Thank you all very much. We will now proceed to questions, and those will have to be kept within seconds of four minutes each or we will shortchange some of our colleagues. Try to keep those questions succinct in an effort to allow for as many questions as possible.

Senator Cardozo: This is an incredible panel before us. Thank you for joining us. I wish we had more time because we could spend an hour, at least, with each of you. I have to pick one or two questions, but there are many more.

Mr. Noël, maybe I will start with you. Thank you for your presentation, sir. With regard to ministerial orders, which is section 7 of the supporting authorized access to information act, or SAAIA, how common are ministerial orders in this kind of situation? To what extent could we have a situation where there can be political abuse of that power? I'm thinking of things that

[*Français*]

Alors que le gouvernement envisage des réformes plus vastes du cadre canadien d'examen et de surveillance, l'office est tout disposé à mettre son expertise à contribution.

[*Traduction*]

En conclusion, les dispositions relatives à la notification contenues dans ce projet de loi, associées à un accès en temps opportun aux renseignements pertinents et au pouvoir discrétionnaire indépendant de l'OSSNR de prioriser ses examens, renforceront notre capacité à évaluer l'utilisation de ces pouvoirs.

[*Français*]

Nos examens indépendants contribuent à faire en sorte que les pouvoirs soient exercés de manière responsable, que les risques soient gérés de façon appropriée et que les institutions canadiennes de sécurité nationale continuent de mériter la confiance que leur accordent les Canadiens.

[*Traduction*]

La réalisation de ces objectifs dépendra d'un financement adéquat et d'une mise à jour législative. Elle continuera aussi d'exiger une culture gouvernementale sensible au rôle essentiel que joue un examen rigoureux pour préserver la confiance dans les activités nécessaires des organismes de renseignement et de sécurité.

[*Français*]

Je vous remercie de votre attention. Nous serons heureux de répondre à vos questions.

[*Traduction*]

La présidente : Je vous remercie tous. Nous allons maintenant passer aux questions, qu'il faudra limiter à quatre minutes chacune, sinon nous priverons certains de nos collègues de la possibilité de s'exprimer. Essayez de formuler des questions concises, afin de permettre le plus grand nombre possible de questions.

Le sénateur Cardozo : Nous avons devant nous un groupe de témoins exceptionnel. Merci d'être venus. J'aimerais que nous ayons plus de temps, car nous pourrions passer au moins une heure avec chacun d'entre vous. Je dois choisir une ou deux questions, mais j'en ai bien d'autres.

Monsieur Noël, je vais peut-être commencer par vous. Je vous remercie de votre exposé, monsieur. En ce qui concerne les arrêtés ministériels, visés à l'article 7 de la Loi sur l'accès à l'information, la LSMAAI, dans quelle mesure sont-ils courants dans ce genre de situation? Dans quelle mesure pourrions-nous nous retrouver dans une situation où ce pouvoir ferait l'objet

have happened in certain other countries where political actors have really gamed the judicial and security systems. What are the possibilities of those kinds of situations happening here, and to what extent do you guard against them? Would you review every ministerial order under this act?

Mr. Noël: Yes, I would.

The experiences over the past five years show that, originating from CSIS and CSE, there are approximately 15 applications per year. They have to be compliant with what the legislation is all about. They cannot invent a new jurisdiction. Their jurisdiction is enumerated. I am looking particularly at this law here, this bill. If you look at the factors at paragraphs 7(3)(a), (b), (c), (d) and (e), you have a list of items. Then it mentions any other factor that the minister considers relevant. If the minister wants to rely on a new factor, the criterion of relevancy has its significance.

To answer directly whether there is a way to ensure that there won't be any abuse in the future, there comes a time when a commissioner must decide that's enough and it is not part of their jurisdiction, or I don't see enough justification to conclude the way the minister wants.

Senator Cardozo: Right. Do you review that decision before it goes into effect, or is it post-facto?

Mr. Noël: It is before.

Senator Cardozo: It is before. Okay.

Mr. Noël: If I don't sign off, there is no order.

Senator Cardozo: For information, does this happen quickly? There is information that security forces have to act on it quickly. Might you get a call in the middle of the night saying, "Can you approve this?"

Mr. Noël: I referred to the number 15, which is my experience.

My experience is that, on a few occasions, there was something that had to be looked at quickly because of the situation. At the time, I reviewed that over a period of 36 hours and made up my mind as to the conclusion. I decided that the justification of my decision would follow.

The Chair: Thank you, Mr. Noël.

[*Translation*]

Senator Martel: Thank you for being here today.

d'abus politique? Je pense à des événements qui se sont produits dans certains autres pays, où des acteurs politiques ont véritablement manipulé les systèmes judiciaire et de sécurité. De telles situations risquent-elles de se produire ici, et dans quelle mesure nous en protégez-vous? Examineriez-vous chaque arrêté ministériel pris en vertu de cette loi?

M. Noël : Oui, je le ferais.

L'expérience des cinq dernières années montre que le SCRS et le CST présentent, en tout, une quinzaine de demandes par an. Elles doivent respecter l'esprit de la loi. Les autorités ne peuvent pas inventer une nouvelle compétence, car leur champ de compétence est précisé. Je m'intéresse particulièrement à cette loi-ci, à ce projet de loi. Si vous regardez les facteurs énoncés aux alinéas 7(3)a), b), c), d) et e), vous avez une liste d'éléments. Il est ensuite question de tout autre facteur que le ministre juge pertinent. Si le ministre souhaite s'appuyer sur un nouveau facteur, le critère de pertinence a son importance.

Pour répondre directement à la question de savoir s'il existe un moyen de garantir qu'il n'y aura pas d'abus à l'avenir, il arrive un moment où un commissaire doit décider que cela suffit et que cela ne relève pas de sa compétence, ou qu'il ne voit pas de justification suffisante pour conclure dans le sens souhaité par le ministre.

Le sénateur Cardozo : Bien. Examinez-vous la décision en question avant son entrée en vigueur ou a posteriori?

M. Noël : Je l'examine avant.

Le sénateur Cardozo : C'est avant. Très bien.

M. Noël : Si je ne donne pas mon accord, il n'y a pas d'arrêté.

Le sénateur Cardozo : À titre d'information, est-ce que cela arrive rapidement? On sait que les forces de sécurité doivent agir rapidement. Pourriez-vous recevoir un appel au milieu de la nuit vous demandant si vous pouvez approuver un arrêté?

M. Noël : J'ai parlé d'une quinzaine de demandes, à ce que j'ai constaté.

D'après mon expérience, il est arrivé à quelques occasions qu'il faille examiner quelque chose rapidement en raison de la situation. Ainsi, j'ai dû examiner un dossier pendant 36 heures et j'en ai tiré ma conclusion. J'ai décidé que la justification de ma décision suivrait.

La présidente : Merci, monsieur Noël.

[*Français*]

Le sénateur Martel : Je vous remercie d'être présents aujourd'hui.

Mr. Noël, you recommended that the government determine whether alternatives exist before issuing confidential orders. As I review the bill today, I still do not see that requirement clearly set out in the legislation. Does that concern remain?

Mr. Noël: Senator Martel, we may need to wait for the regulations, as a whole regulatory framework will follow the bill. That said, if the minister were not to justify why he is proceeding on a confidential rather than a public basis, in my view that would raise an important question on which the commissioner would have to rule. Why? Because, as a matter of principle, a decision-maker, a minister, must act publicly. It is only in exceptional circumstances that a minister may act confidentially. So that would be one of the factors supporting my recommendation that proportionality form part of the decision-making process, in order to ensure that the exercise of these powers is subject to meaningful review.

Senator Martel: Mr. Noël, if the minister isn't required to consider alternatives, how can you ensure that a ministerial order is truly necessary?

Mr. Noël: I have spent 48 years working in matters involving classified information, as a lawyer, as a judge and now as commissioner. At a certain point, when you sense that something isn't working, you have to act. I believe that, if I were faced with such a situation, I would act.

Senator Martel: Mr. Dufresne, Bill C-22 would allow certain electronic service providers to be required to retain categories of metadata for periods of up to six months. I understand that this information may be useful for investigative purposes, but it is also important to ensure that Canadians' privacy is properly protected. In your view, do the safeguards currently provided for in the bill strike an appropriate balance between the needs of investigators and the protection of personal information?

Mr. Dufresne: In my view, that objective is achieved through the principles of necessity and proportionality. This requires that, when an order is issued or a regulation is made, an assessment be carried out: Is it absolutely essential or necessary? The House added an essentiality requirement in the case of regulations, but one must also ask whether the measure is proportionate. What impact will it have on privacy or cybersecurity? What risks will it entail? Is it too lengthy or too intrusive? It is fundamental to consider all of these factors. This is a cornerstone of privacy protection. Even when the National Security and Intelligence Committee of Parliamentarians conducted its 2025 review of lawful access in this area, it recommended a legal framework incorporating fundamental principles such as necessity and proportionality, which is what Bill C-22 proposes.

Senator Martel: Thank you, Mr. Dufresne, Mr. Noël.

Monsieur Noël, vous avez demandé au gouvernement de vérifier s'il existe d'autres solutions avant de rendre un arrêt confidentiel. Aujourd'hui, lorsque je consulte le projet de loi, je ne vois toujours pas cette obligation clairement écrite. Cette préoccupation demeure-t-elle?

M. Noël : Sénateur Martel, il faudra peut-être attendre les règlements, car toute une réglementation suivra le projet de loi. Cela dit, si jamais le ministre ne justifiait pas la raison pour laquelle il procède confidentiellement et non publiquement, à mon avis, cela soulèverait une question importante sur laquelle le commissaire devrait se prononcer. Pourquoi? Parce que, en principe, un décideur, un ministre doit agir publiquement. Ce n'est qu'exceptionnellement qu'il peut agir confidentiellement. Ce serait alors l'un des éléments, et cela vient appuyer ma recommandation que la proportionnalité fasse partie du processus de décision pour s'assurer et garantir que l'exercice sera véritablement vérifié.

Le sénateur Martel : Monsieur Noël, si le ministre n'est pas tenu d'examiner les autres solutions, comment pouvez-vous vous assurer qu'un arrêt ministériel est vraiment nécessaire?

M. Noël : Cela fait 48 ans que j'agis dans le domaine secret comme avocat, comme juge, et maintenant comme commissaire. À un moment donné, quand on sent que quelque chose ne fonctionne pas, on doit agir. Je crois que si j'étais devant une situation semblable, j'agirais.

Le sénateur Martel : Maître Dufresne, le projet de loi C-22 permettrait d'obliger certains fournisseurs de services électroniques de conserver des catégories de métadonnées pour une période pouvant aller jusqu'à six mois. Je comprends que ces informations peuvent être utiles dans le cadre d'enquêtes, mais il faut aussi s'assurer de bien protéger la vie privée des Canadiens. Selon vous, les garanties prévues actuellement dans le projet de loi permettent-elles de trouver un juste équilibre entre les besoins des enquêteurs et la protection des renseignements personnels?

Me Dufresne : Selon moi, on atteint cet objectif avec le critère de nécessité et de proportionnalité. Cela exige que, lorsqu'on émet une ordonnance, lorsqu'on adopte un règlement, une évaluation soit de mise : est-ce absolument essentiel ou nécessaire? Il y a un élément du facteur essentiel qui a été ajouté par la Chambre pour les règlements, mais aussi, est-ce proportionnel? Quel est le préjudice à la vie privée ou à la cybersécurité? Quels sont les risques qui en découleront? Est-ce trop long ou trop intrusif? Il est fondamental de considérer tout cela. C'est un pilier de la vie privée. Même quand le Comité des parlementaires sur la sécurité nationale et le renseignement a fait sa revue en 2025 sur l'accès légal dans ce secteur, ils ont recommandé un régime juridique qui inclut des principes fondamentaux, comme la nécessité et la proportionnalité, ce qui est proposé par le projet de loi C-22.

Le sénateur Martel : Merci, maître Dufresne et monsieur Noël.

[*English*]

The Chair: Thank you. I welcome Senator Youance from Quebec and Senator Yussuff from Ontario. Thank you for joining us.

Senator Patterson: This is a distinguished panel. This is probably a question that touches on privacy and potentially NSIRA as well.

We know that Bill C-22 proposes to improve the ability of law enforcement and national security agencies to obtain certain telecommunications information.

However, we also know that the government has presented an example involving a missing 16-year-old whose last known cellphone location could not be obtained from the service provider. It caused delays in the search. Of course, in this case, it is with regard to a life. It isn't necessarily the example of what I'm providing to you. It's access to information.

This bill establishes a framework for lawful access by law enforcement and CSIS. However, in search and rescue operations, it can involve several organizations, including police services, both federal, provincial and municipal; emergency management authorities; volunteer search and rescue organizations; and the Canadian Armed Forces.

If the bill's stated purpose is to modernize the gathering and production of data and information during investigations, its provisions identify law enforcement and intelligence authorities only rather than creating a direct-access mechanism for volunteer search and rescue organizations.

From an oversight perspective — and this may be to NSIRA first — is there a need for clearer statutory guidance on which authorities may request location information from telecommunication providers during a search and rescue emergency, especially when minutes and hours could mean a life?

Mr. Forcese: Thank you for the question. We don't have a view on the breadth of the current law. However, insofar as we're talking about a federal agency, from a review retrospective perspective, we would have jurisdiction to review the use of any information that might be acquired under Bill C-22 by anyone in the federal enterprise. It would not reach those in provincial jurisdictions, but under the federal enterprise, it wouldn't be confined only to law enforcement and intelligence services.

[*Traduction*]

La présidente : Merci. Je souhaite la bienvenue à la sénatrice Youance, du Québec, et au sénateur Yussuff, de l'Ontario. Merci de vous joindre à nous.

La sénatrice Patterson : Nous avons un groupe d'éminents témoins. Il s'agit probablement d'une question qui concerne la vie privée et potentiellement aussi l'OSSNR.

Nous savons que le projet de loi C-22 propose d'améliorer la capacité des organismes d'application de la loi et des agences de sécurité nationale d'obtenir certains renseignements en matière de télécommunications.

Cependant, nous savons aussi que le gouvernement a présenté un exemple concernant un adolescent de 16 ans porté disparu, dont la dernière localisation connue du cellulaire n'a pas pu être obtenue auprès du fournisseur de services. Cela a entraîné des retards dans les recherches. Bien sûr, dans ce cas, il s'agit d'une vie humaine. Cet exemple n'illustre pas forcément ce dont je vous parle, c'est-à-dire l'accès à l'information.

Le projet de loi établit un cadre destiné à régir l'accès légal à l'information par les organismes d'application de la loi et le SCRS. Cependant, dans des opérations de recherche et de sauvetage, plusieurs organismes peuvent intervenir, dont les services de police fédéraux, provinciaux et municipaux, les autorités chargées de la gestion des situations d'urgence, les organismes de recherche et de sauvetage bénévoles, ainsi que les Forces armées canadiennes.

Si l'objet déclaré du projet de loi est de moderniser la collecte et la communication de données et de renseignements au cours des enquêtes, ses dispositions ne visent que les organismes d'application de la loi et les agences de renseignement, et ne créent pas de mécanisme d'accès direct pour les organismes de recherche et de sauvetage bénévoles.

Du point de vue de la surveillance — et la question s'adresse peut-être d'abord à l'OSSNR —, faut-il des directives législatives plus claires sur les autorités habilitées à demander des renseignements de localisation aux fournisseurs de services de télécommunications dans une opération de recherche et de sauvetage menée d'urgence, surtout lorsque chaque minute, chaque heure qui passe met une vie en danger?

M. Forcese : Je vous remercie de cette question. Nous n'avons pas d'avis sur la portée de la loi actuelle. Toutefois, dans la mesure où nous parlons d'un organisme fédéral, d'un point de vue rétrospectif, nous aurions compétence pour examiner l'utilisation de toute information qui pourrait être obtenue en vertu du projet de loi C-22 par quiconque au sein de l'appareil fédéral. Cela ne s'étendrait pas aux administrations provinciales, mais dans l'appareil fédéral, cela ne se limiterait pas aux seuls organismes d'application de la loi et de renseignement.

National security and intelligence are a remit not tied to specific institutions.

Senator Patterson: Got it. Thank you.

If I can follow up with our Privacy Commissioner, if the RCMP or the Canadian Armed Forces are obtaining location information in support of a search and rescue operation, what oversight should apply to the subsequent use of that information and data?

Mr. Dufresne: The bill aims to provide that regime in terms of what is disclosed and what is limited; that's why we are advocating for necessity and proportionality, saying not to take more than you need and ensure you go before a judge if you will be dealing with more sensitive information, as the Supreme Court has highlighted.

In terms of emergency actions and situations where time is of the essence, there are some exceptions provided in the legislation, including privacy legislation, where information could be disclosed.

Senator Patterson: I will stop there. Thank you.

Senator Pate: Mr. Dufresne, my first question is for you.

As you might be aware, First Nations children's advocate Cindy Blackstock was the subject of online surveillance by a federal government department acting without a warrant, which the Canadian Human Rights Commission ruled to be retaliation. The Privacy Commissioner ruled it to be a violation of the spirit of the Privacy Act in 2013.

Surveillance extended not just to Ms. Blackstock but to those with whom she interacted, including First Nations children.

I'm curious as to whether there is anything — I couldn't find anything — in Bill C-22 that would provide the type of injunctive relief that was not available to Ms. Blackstock in that instance. Also, what measures in Bill C-22 would prevent what happened to Ms. Blackstock from occurring again to others, including other Indigenous political advocates as well as land and water protectors?

Mr. Dufresne: In the context of this bill, you would look at some remedies from a criminal law standpoint or from a national security standpoint. Is the evidence that has been obtained improper? If so, it wouldn't be used in court. It would be quashed. There would be remedies of that nature.

La sécurité nationale et le renseignement relèvent d'un mandat qui n'est pas lié à des institutions particulières.

La sénatrice Patterson : Je comprends. Merci.

Si je peux poser une question complémentaire au commissaire à la protection de la vie privée : si la GRC ou les Forces armées canadiennes obtiennent des données de localisation à l'appui d'une opération de recherche et de sauvetage, quel contrôle devrait s'appliquer à l'utilisation ultérieure de ces renseignements et de ces données?

Me Dufresne : Le projet de loi vise à établir ce régime en précisant ce qui peut être communiqué et ce qui doit l'être de façon limitée. C'est pourquoi nous préconisons les principes de nécessité et de proportionnalité, autrement dit que l'on ne doit prendre que ce dont on a besoin et veiller à se présenter devant un juge si l'on doit traiter des renseignements plus sensibles, comme l'a souligné la Cour suprême.

En ce qui concerne les mesures et les situations d'urgence où le temps est compté, la législation, y compris les lois sur la protection des renseignements personnels, prévoit certaines exceptions qui permettent de communiquer des renseignements.

La sénatrice Patterson : Je m'arrêterai là. Merci.

La sénatrice Pate : Maître Dufresne, ma première question s'adresse à vous.

Comme vous le savez peut-être, Cindy Blackstock, défenseure des enfants des Premières Nations, a fait l'objet d'une surveillance en ligne de la part d'un ministère fédéral agissant sans mandat, ce que la Commission canadienne des droits de la personne a qualifié de mesure de représailles. Le commissaire à la protection de la vie privée a statué en 2013 qu'il s'agissait d'une violation de l'esprit de la Loi sur la protection des renseignements personnels.

La surveillance ne visait pas seulement Mme Blackstock. Elle s'étendait aux personnes avec lesquelles elle interagissait, y compris des enfants des Premières Nations.

Je me demande s'il y a quoi que ce soit — je n'ai rien trouvé — dans le projet de loi C-22 qui permettrait d'obtenir le type d'injonction que n'a pas pu demander Mme Blackstock dans ce cas précis. Par ailleurs, quelles mesures prévues dans le projet de loi C-22 empêcheraient que ce qui est arrivé à Mme Blackstock arrive à d'autres personnes, notamment à d'autres défenseurs politiques autochtones, ainsi qu'à des protecteurs des terres et de l'eau?

Me Dufresne : Dans le contexte de ce projet de loi, il faudrait examiner certains recours sous l'angle du droit pénal ou de la sécurité nationale. Les preuves obtenues sont-elles irrégulières? Si tel est le cas, elles ne seraient pas admises devant un tribunal. Elles seraient annulées. Il existerait des recours de cette nature.

Bill C-22 aims to create this. In what situations can you get the information without an order from a judge, and in what situations is such an order required? That is why we focused some of our recommendations on the definition. To whom can you go for these types of information? Don't make it too broad. Make it necessary and proportionate, and ensure that any type of information or any type of surveillance, when it is proposed, is scrutinized. Privacy and being free from surveillance are key elements of a free and democratic society.

At the same time, we need to ensure law enforcement has the tools it needs. As the Supreme Court has confirmed in the *Bykovets* case — and as I've argued — it should not be a zero-sum game: Canadians deserve security and law enforcement as well as the fundamental right to privacy.

Senator Pate: Issues have also been raised by the Ontario Human Rights Commission regarding Black Canadians, particularly in Toronto. Are there any measures in Bill C-22 that would prevent existing patterns of discriminatory over-surveillance and over-policing of Black, Indigenous and other marginalized groups from being reinforced by this legislation?

Mr. Dufresne: If the concern is discriminatory approaches by any organ of government, then the Human Rights Commission and, potentially, courts would be the appropriate mechanisms. In this bill, I think I would see the role of the judges reviewing the orders that are sought as being very critical. If we're dealing with regulation-making powers, that's where the criteria of necessity and proportionality focus on privacy and security — being very diligent in reviewing any proposed exercise of power.

Senator Pate: Thank you.

Senator Dhillon: Commissioner Dufresne, I will direct this question to you.

You have identified the need and the importance of the approach being necessary and proportionate. The legislation requires the minister to consider a range of factors, including the benefits to investigations, technical feasibility, costs, privacy and cybersecurity. Ministerial orders are also subject to approval by the Intelligence Commissioner.

I want to understand what additional protections your proposed amendment would provide beyond those existing safeguards. Could you give us an example of a technical

Le projet de loi C-22 vise à instaurer cela. Dans quelles situations peut-on obtenir ces renseignements sans ordonnance d'un juge, et dans quelles situations une telle ordonnance est-elle requise? C'est pourquoi nous avons axé certaines de nos recommandations sur la définition. À qui peut-on s'adresser pour obtenir ce type de renseignements? Il ne faut pas que la définition soit trop large. Il faut que ce soit nécessaire et proportionné, et il faut veiller à ce que tout type de renseignement ou de surveillance, lorsqu'il est proposé, fasse l'objet d'un examen minutieux. La protection de la vie privée et le fait d'être à l'abri de la surveillance sont des éléments clés d'une société libre et démocratique.

Parallèlement, nous devons veiller à ce que les forces de l'ordre disposent des outils dont ils ont besoin. Comme l'a confirmé la Cour suprême dans l'affaire *Bykovets* — et comme je l'ai fait valoir —, ce ne devrait pas être un jeu à somme nulle : les Canadiens ont droit à la sécurité et à l'application de la loi, et ils ont le droit fondamental au respect de leur vie privée.

La sénatrice Pate : La Commission ontarienne des droits de la personne a également soulevé des questions concernant les Canadiens noirs, en particulier à Toronto. Le projet de loi C-22 prévoit-il des mesures qui empêcheraient que ce projet de loi ne renforce les pratiques existantes de surveillance et d'intervention policières excessives et discriminatoires à l'égard des Noirs, des Autochtones et d'autres groupes marginalisés?

Me Dufresne : Si le problème réside dans des pratiques discriminatoires de la part d'un organe quelconque du gouvernement, la Commission des droits de la personne et, éventuellement, les tribunaux seraient les mécanismes appropriés. Dans ce projet de loi, le rôle des juges chargés d'examiner les ordonnances demandées est, à mon sens, essentiel. Lorsqu'il s'agit de pouvoirs de réglementation, c'est là que les critères de nécessité et de proportionnalité axés sur la protection de la vie privée et la sécurité entrent en jeu, et il faut faire preuve d'une grande rigueur dans l'examen de tout exercice proposé de ces pouvoirs.

La sénatrice Pate : Merci.

Le sénateur Dhillon : Commissaire Dufresne, je vous adresse cette question.

Vous avez souligné la nécessité et l'importance d'une approche fondée sur les principes de nécessité et de proportionnalité. Le projet de loi prévoit que le ministre doit tenir compte d'une série de facteurs, comme les avantages pour les enquêtes menées, la faisabilité technique, les coûts, la protection de la vie privée et la cybersécurité. Les arrêtés ministériels sont également soumis à l'approbation du commissaire au renseignement.

J'aimerais comprendre quelles protections supplémentaires la modification que vous proposez apporterait au-delà des mesures de protection existantes. Pouvez-vous nous donner un exemple

obligation that might satisfy the current statutory requirements, including independent approval, that you believe should nevertheless be prohibited under your proposed necessarily and proportionality test?

Mr. Dufresne: Thank you, senator.

In my view, a clear reference to proportionality, in particular, is missing. That is absent from the elements that must be considered. The House has added an element of the essential nature, so that goes to necessity, so there are some elements there. However, it is the two of them. It is making sure that, when issuing an order in terms of retention — what you're going to ask ESPs to retain or what types of systems you put in place for how long and so on — you need to establish that it is needed for the operations of the state. That's important, and that was one that the National Security and Intelligence Committee of Parliamentarians talked about. Sometimes, there's a gap in data collection or evidence in terms of how many cases are needed and so on.

Also, we need to look at whether it is proportionate. Are we causing too much harm to privacy or cybersecurity? And cybersecurity is a growing issue in that the longer you retain data, the more there is a risk that there can be bad actors gaining access.

So, necessity and proportionality really get to those two things. They will help make sure, in my view, that the decision is going to be safer and more protective of privacy while, at the same time, allowing authorities to do their work.

Senator Dhillon: Regarding those two principles, do you believe it is important that they be captured in legislation, or do you feel comfortable and have confidence that they might be displayed within the regulatory framework?

Mr. Dufresne: I'm not the one who would be overseeing those regulations; Commissioner Noël would be. If the legislation doesn't require something to be considered, it is hard for an authority to say that it should have been considered. "I am not seeing information on this element, so, therefore, I cannot approve it." So having it in the legislation is —

Of course, the minister can certainly consider those things, and the legislation does mention any other relevant factors. One would hope that is the spirit.

Given the importance of this — and I did note this, and I repeat it now — the NSICOP explicitly named this, and international privacy authorities around the world consistently refer to necessity and proportionality. It is consistent with the approach under the Charter. When we are justifying a Charter violation under section 1, we are looking at whether it minimally impairs the right that is being impacted.

d'obligation technique qui pourrait satisfaire aux exigences légales actuelles, y compris l'approbation indépendante, mais qui, selon vous, devrait néanmoins être interdite en vertu de votre critère de nécessité et de proportionnalité?

Me Dufresne : Merci, sénateur.

À mon avis, il manque notamment une mention claire de la proportionnalité. Celle-ci est absente des éléments qui doivent être pris en compte. La Chambre a ajouté un élément essentiel, qui est la nécessité. Il y a donc des éléments à cet égard. Cependant, ce sont les deux éléments à la fois. Il s'agit de s'assurer que, lorsque l'on rend une ordonnance de conservation — ce que l'on va demander aux fournisseurs de services de courriel, les FSC, de conserver ou quels types de systèmes on met en place, pour combien de temps, etc. —, c'est nécessaire au bon fonctionnement de l'État. C'est important, et c'est un point dont le Comité des parlementaires sur la sécurité nationale et le renseignement a parlé. Parfois, il y a des lacunes dans la collecte de données ou de preuves quant au nombre de cas nécessaires, etc.

De plus, il faut voir si la mesure est proportionnée. Portons-nous trop atteinte à la vie privée ou à la cybersécurité? Et la cybersécurité est un enjeu croissant, car plus on conserve longtemps les données, plus le risque est grand que des acteurs malveillants y aient accès.

La nécessité et la proportionnalité portent donc vraiment sur ces deux aspects. À mon avis, elles contribueront à garantir que la décision soit plus sûre et qu'elle protège davantage la vie privée, tout en permettant aux autorités de faire leur travail.

Le sénateur Dhillon : En ce qui concerne ces deux principes, croyez-vous qu'il soit important qu'ils soient inscrits dans le projet de loi, ou pensez-vous qu'ils puissent être intégrés au cadre réglementaire et que cela suffirait?

Me Dufresne : Ce ne sera pas à moi de superviser ces règlements, mais au commissaire Noël. Si la loi n'exige pas qu'un élément soit pris en compte, il est difficile pour une autorité de dire qu'il aurait fallu en tenir compte. « Je ne vois pas d'information sur cet élément; par conséquent, je ne peux pas l'approuver. » Donc, en l'incluant dans le projet de loi...

Bien sûr, le ministre peut certainement tenir compte de ces éléments, et le projet de loi parle effectivement de tout autre facteur pertinent. On espère que tel est l'esprit.

Compte tenu de l'importance de cette question — je l'ai déjà souligné, et je le répète maintenant —, le Comité des parlementaires sur la sécurité nationale et le renseignement l'a mentionnée explicitement, et les autorités internationales en matière de protection de la vie privée renvoient systématiquement à la nécessité et à la proportionnalité. C'est conforme à l'approche prévue par la Charte. Lorsque nous justifions une violation de la Charte en vertu de l'article premier,

So, I would see no harm in adding it in the legislation, and I would see benefits in reassuring Canadians and industry that those orders are going to be as tailored as they need to be.

Senator Yussuff: Thanks to the witnesses, and I'm sorry for being late. Other things are going on in this place, as usual.

Let me get to the question that's on many Canadians' minds. As you know, a number of iterations of this bill didn't make it this far, but we're here now. Much has been learned in the process of coming to this final chapter, if we get there; obviously, that's the hope.

Given what our Five Eyes allies have done ahead of us in regard to similar legislation, what can you share that is valuable for us to understand? Obviously, there is variance, and we have the Charter. They might not have something like that in some of the countries. What is the variance between the other legislation that might be of value for Canadians who are still wondering whether this bill is overreaching its intended purpose? I will start with Mr. Dufresne and then move to Mr. Noël.

Mr. Dufresne: I'll address two elements that regard Part 2 of the bill in terms of requiring service providers to put in place tools and mechanisms.

If we look at Australia or the U.K., they have incorporated a necessity and proportionality assessment in their legislation. That is instructive in terms of the types of international consensus, the importance of those principles and how useful they are. Likewise, Australia, the United Kingdom and New Zealand have put in place some mechanisms that I've recommended in my fifth recommendation for providers to be able to pre-emptively request an assessment by an independent technical expert if they have concerns that what is being asked of them will result in systemic vulnerabilities.

So, these are good practices, and they could help allay some of the concerns that have been voiced in the context of this bill in terms of whether we will be inadvertently causing systemic vulnerability, creating back doors and so on. The government has stated that's not the intention. If there are still remaining concerns, that mechanism would help allay them.

nous cherchons à déterminer si cette violation porte atteinte, ne serait-ce que de manière minime, au droit concerné.

Je ne vois donc aucun inconvénient à l'ajouter dans le projet de loi, et j'y vois des avantages pour ce qui est d'assurer aux Canadiens et à l'industrie que ces arrêtés et ces ordonnances seront aussi adaptés que nécessaire.

Le sénateur Yussuff : Je remercie les témoins, et je suis désolé d'être en retard. Comme d'habitude, il se passe d'autres choses au Sénat.

Permettez-moi de poser la question qui préoccupe de nombreux Canadiens. Comme vous le savez, plusieurs versions de ce projet de loi ne sont pas arrivées jusqu'à cette étape, mais nous y sommes maintenant. Nous avons beaucoup appris au cours du processus qui nous mène à ce chapitre final, si nous y parvenons, et c'est évidemment ce que nous espérons.

Compte tenu de ce que nos alliés du Groupe des cinq ont fait avant nous en matière de loi semblable, que pouvez-vous nous dire qui nous aiderait à mieux comprendre? Évidemment, il y a des différences, et nous avons la Charte. Certains de ces pays n'ont peut-être rien de comparable. Quelles sont les différences par rapport aux autres lois qui pourraient être utiles aux Canadiens qui se demandent encore si ce projet de loi va au-delà de son objectif initial? Je commencerai par Me Dufresne, puis je passerai à M. Noël.

Me Dufresne : Je parlerai de deux éléments relatifs à la partie 2 du projet de loi qui concernent l'obligation pour les fournisseurs de services de mettre en place des outils et des mécanismes.

Si l'on prend l'exemple de l'Australie ou du Royaume-Uni, ces pays ont inscrit dans leur loi une évaluation de la nécessité et de la proportionnalité. C'est instructif quant aux types de consensus internationaux, à l'importance de ces principes et à leur utilité. De même, l'Australie, le Royaume-Uni et la Nouvelle-Zélande ont mis en place des mécanismes que je recommande dans ma cinquième recommandation, afin que les fournisseurs puissent demander de manière préventive une évaluation par un expert technique indépendant, s'ils craignent que ce qu'on leur demande entraîne des vulnérabilités systémiques.

Il s'agit donc de bonnes pratiques, qui pourraient contribuer à apaiser certaines des préoccupations exprimées dans le contexte de ce projet de loi, notamment pour ce qui est de savoir si nous risquons de causer involontairement une vulnérabilité systémique, de créer des portes dérobées, et ainsi de suite. Le gouvernement a déclaré que ce n'était pas son intention. Si des préoccupations subsistent, ce mécanisme aiderait à les apaiser.

Mr. Noël: In terms of metadata in Australia, I think the retention can be over two years. That's one aspect. I think the six months in this bill is the shortest period of retention out of the Five Eyes partners.

As for the Americans, it is hard to know how they operate. It's all very well, but I'm intrigued. I've been trying to research that and find out exactly how they operate. I know there is the FISA Court. I met the judges. I also know there are presidential executive orders that are confidential and we're not aware of. I understand that some American senators criticized this bill, but it is hard to know where they are coming from. What I'm trying to get at is that it is hard to understand the Americans. They have the core service providers in their country. This is my personal opinion, but I suspect that there are a lot of arrangements we're not aware of.

As for Great Britain, I agree with the Privacy Commissioner that necessity and proportionality are clearly mentioned in their legislation, as they should be in ours.

Let me give you a final thought on that: Proportionality means justification. It means when you have opposing goals, as you do in paragraphs 7(3)(a), 7(3)(d) and 7(3)(e), the decision maker must ask, "How am I balancing this?" Is it in the interest of the criminal investigation, or is it in the interest of the users? Does it impact their privacy too much? How does the minister deal with that?

Through my present role, I have seen that. It is working. They have to justify their decisions. Justifying means a lot. It means that you must put your opinion forward.

Senator Hay: Thank you all for being here. I'm going to throw this out as a free-for-all, so whoever wants to answer can. I am on a little bit of a learning mission here, and I'm trying to understand where Bill C-22 may apply with unintended consequences around data, privacy, security and cybersecurity. I'm going to give you a real example.

I used to work in an organization that was deeply involved with data and technology, as well as youth and mental health. I worked with some of the more vulnerable young people coast to coast to coast nationally. I'm curious how Bill C-22 would apply to that data. The organization holds a lot of data, including transcript data, young people's data and locations, with up to 3 million to 4 million interactions a year. Maybe it doesn't apply, but that would be helpful to know. I'm pretty sure people would want to know the difference because this is all based on trust. This is confidential and anonymous.

M. Noël : En ce qui concerne les métadonnées en Australie, je crois que la période de conservation peut dépasser deux ans. C'est un aspect. La période de six mois prévue dans le projet de loi est, me semble-t-il, la plus courte parmi les partenaires du Groupe des cinq.

Quant aux Américains, il est difficile de savoir comment ils fonctionnent. Tout cela est très bien, mais je suis perplexe. J'ai essayé de faire des recherches à ce sujet pour découvrir exactement comment ils opèrent. Je sais qu'il y a la Foreign Intelligence Surveillance Court. J'ai rencontré les juges. Je sais aussi qu'il existe des décrets présidentiels confidentiels dont nous n'avons pas connaissance. Je crois savoir que certains sénateurs américains ont critiqué le projet de loi, mais il est difficile de cerner leur point de vue. Ce que j'essaie de dire, c'est qu'il est difficile de comprendre les Américains. Ils ont sur leur territoire les principaux fournisseurs de services. C'est mon avis personnel, mais je soupçonne qu'il existe de nombreuses ententes dont nous n'avons pas connaissance.

Pour ce qui est de la Grande-Bretagne, je suis d'accord avec le commissaire à la protection de la vie privée : les principes de nécessité et de proportionnalité sont clairement mentionnés dans la loi britannique, comme ils devraient l'être dans la nôtre.

Permettez-moi une dernière réflexion à ce sujet : qui dit proportionnalité dit justification. Autrement dit, lorsque l'on a des objectifs contradictoires, comme c'est le cas aux alinéas 7(3)a), 7(3)d) et 7(3)e), le décideur doit se demander comment concilier ces éléments. Est-ce dans l'intérêt de l'enquête criminelle ou dans l'intérêt des utilisateurs? Est-ce que cela porte-t-il trop atteinte à leur vie privée? Comment le ministre gère-t-il cela?

Dans le cadre de mes fonctions actuelles, j'ai pu le constater. Ils doivent justifier leurs décisions, ce qui est très important. Cela signifie que l'on doit faire valoir son point de vue.

La sénatrice Hay : Merci à tous d'être ici. J'adresserai cette question à tous les témoins, afin que qui souhaite y répondre puisse le faire. Je suis ici, en quelque sorte, pour apprendre, et j'essaie de comprendre dans quelles circonstances le projet de loi C-22 pourrait s'appliquer et avoir des conséquences indésirables sur les données, la protection de la vie privée, la sécurité et la cybersécurité. Permettez-moi de vous donner un exemple concret.

J'ai travaillé pour un organisme œuvrant auprès des jeunes dans le domaine de la santé mentale, qui est très concerné par les données et la technologie. J'ai travaillé avec des jeunes parmi les plus vulnérables, d'un bout à l'autre du pays. Je me demande comment le projet de loi C-22 s'appliquerait à leurs données. Cet organisme détient beaucoup de données, notamment des transcriptions de conversations et des renseignements sur les jeunes et l'endroit où ils se trouvent. Il a jusqu'à 3 à 4 millions d'interactions par année. Peut-être que le projet de loi ne s'applique pas à cet organisme, mais il serait utile de le savoir. Je

Occasionally, there would be a situation in this organization where we would work with the RCMP because of the potential for self-harm, when there were public threats to a school or if there may be harm to others.

My question is this: What risk would young people take if they reached out to this organization that now holds their data? Does this mean the organization might be asked or required to give the government data from young people in Iqaluit or Ontario? Under Bill C-22, if this organization had to comply, would it create more risk of cyberattacks to capture this data?

Mr. Dufresne: I can quickly start. This touches on the scope of what is captured under Bill C-22 and for what types of powers. If we look at the power to confirm a service demand — that's where a peace officer would ask a provider for confirmation — it is limited to a telecommunication service provider. To me, it doesn't sound like what you described would be covered.

Senator Hay: Except the provision at this organization is through telecommunications.

Mr. Dufresne: Right, but the organization itself is not a telecommunications service provider. However, the power to obtain subscriber information when going to a judge is not limited to telecommunications service providers. It is open to a person who provides services to the public, so that's one of the concerns that I've identified.

In our view, that, too, should be limited to a telecommunications service provider so that the scope is limited to the type of basic subscriber information we're thinking about in this context. The confirmation of service demands has a carve-out for medical and privileged information, which could apply here, but that carve-out does not apply to the subscriber information requests. In my view, those two things should apply to both exercises of power.

Senator Hay: There are many organizations like the one I'm referring to. Thank you for that. That's very helpful.

I now have a broad question on this bill itself. Do you think it was built in, let's say, a different era or designed for a different time? I'm thinking about AI. This is just an "in your opinion" question.

suis presque certaine que les gens voudraient connaître la différence, car tout cela est une question de confiance. Ces renseignements sont confidentiels et anonymes.

Il nous est arrivé, dans cet organisme, de collaborer avec la GRC en raison d'un risque d'automutilation, de menaces publiques contre une école ou d'un danger potentiel pour autrui.

Ma question est la suivante : à quel risque les jeunes seraient-ils exposés s'ils s'adressaient à cet organisme, qui détient actuellement leurs données? Pourrait-il être contraint de fournir au gouvernement des données concernant des jeunes d'Iqaluit ou de l'Ontario? Et s'il devait se conformer aux exigences prévues dans le projet de loi C-22, risquerait-il davantage de subir des cyberattaques visant à voler ces données?

Me Dufresne : Je vais vous répondre en premier. Cela concerne la portée du projet de loi C-22 et les types de pouvoirs qu'il prévoit. Si l'on prend le pouvoir de demander la confirmation de la fourniture de services — c'est-à-dire lorsqu'un agent de la paix demandera cette confirmation à un fournisseur —, cette demande ne pourra être faite qu'à des fournisseurs de services de télécommunications. À mon avis, ce que vous décrivez ne semble pas être visé.

La sénatrice Hay : Sauf que mon organisme utilise les télécommunications pour fournir des services.

Me Dufresne : C'est vrai, mais l'organisme lui-même n'est pas un fournisseur de services de télécommunications. En revanche, le pouvoir d'obtenir des renseignements relatifs à l'abonné en passant par un juge ne s'exerce pas uniquement à l'égard des fournisseurs de services de télécommunications. Toute personne fournissant des services au public est concernée; et c'est donc l'une des préoccupations que j'ai soulevées.

Selon nous, ce pouvoir ne devrait lui aussi être exercé qu'à l'égard des fournisseurs de services de télécommunications, afin de restreindre la portée au type de renseignements de base relatifs à l'abonné auquel nous pensons dans ce contexte. Il existe une exception concernant les renseignements médicaux et les renseignements protégés par un privilège pour les ordres de confirmer la fourniture de services, et elle pourrait s'appliquer à votre organisme, mais elle ne concernerait pas les demandes de renseignements relatifs à l'abonné. À mon avis, ces deux restrictions devraient s'appliquer aux deux types d'exercice de pouvoir.

La sénatrice Hay : Il existe de nombreux organismes comme celui dont je viens de parler. Merci de votre réponse. Elle est très utile.

À présent, j'ai une question d'ordre général sur le projet de loi lui-même. Pensez-vous qu'il ait été conçu, disons, à une autre époque ou pour d'autres temps? Je pense à l'IA. Je vous demande juste votre opinion.

Mr. Noël: Your question is appropriate. Things are moving so quickly out there. I certainly hope this bill covers it, but I would suggest you ask the minister that question. I think he'd be in a better position to answer that.

Senator McNair: Thank you to the witnesses for being here tonight. We will have some witnesses before our committee who will talk about the onerous side of collecting and retaining the metadata and the risk of holding that metadata. As you know, the other place made an amendment to reduce the metadata retention period from one year to six months.

Mr. Dufresne, do the concepts of proportionality and necessity that you're proposing be put into this legislation, like what has been done with other similar legislation, balance that concern, or should we be reducing the time period even further?

Mr. Dufresne: I'm not recommending a reduction of time. The maximum retention time has been reduced to six months, and I take no issue with that. In my view, necessity and proportionality would address concerns on a case-by-case basis. Not all cases are going to require that six months. Some will require less. But if there is a case that does need it, there should be that possibility.

Senator McNair: Honourable Mr. Noël, do you have anything to add?

Mr. Noël: I think the commissioner answered well.

Senator Cardozo: We talked about two terms, and I'm wondering if you could say a bit more. One is the necessity of proportionality. To what extent is that a rather subjective term, and is there enough in the bill or does that get defined during the course of jurisprudence or decisions that are made?

Mr. Noël: To your first question, these are principles of law. They've been developed through jurisprudence going back centuries. Proportionality goes back to the Greek times.

It is not something new. It is used, senator, on a daily basis in administrative law. The public officer has to justify their decision. The way to do it is to be able to analyze the factors even when they are in contradiction.

I go back to the benefits of the order to the administration of justice; that's the purpose. However, at the same time, what will the potential impact be on the persons to whom the electronic provider supplies the services, or the potential impact on privacy?

M. Noël : C'est une bonne question. Les choses évoluent très rapidement dans ce domaine. J'espère sincèrement que le projet de loi couvre ce sujet, mais je vous suggère de poser cette question au ministre. Je pense qu'il sera mieux à même d'y répondre.

Le sénateur McNair : Je remercie les témoins de leur présence ce soir. Notre comité entendra des témoins qui parleront du côté contraignant de la collecte et de la conservation des métadonnées, ainsi que des risques associés à leur détention. Comme vous le savez, l'autre Chambre a adopté un amendement visant à ramener la période de conservation des métadonnées d'un an à six mois.

Maître Dufresne, les principes de proportionnalité et de nécessité que vous proposez d'intégrer dans ce projet de loi — comme cela a été fait dans d'autres lois comparables — répondent-ils à cette préoccupation, ou devrions-nous réduire encore davantage cette période?

Me Dufresne : Je ne recommande pas de réduire la période de conservation. La période maximale a été ramenée à six mois, et cela ne me pose aucun problème. À mon avis, les principes de nécessité et de proportionnalité nous permettraient de répondre aux préoccupations au cas par cas. Tous les cas ne nécessiteront pas ces six mois. Certains en nécessiteront moins, mais si un cas l'exige, la possibilité sera là.

Le sénateur McNair : Monsieur Noël, avez-vous quelque chose à ajouter?

M. Noël : Je pense que le commissaire a bien répondu à cette question.

Le sénateur Cardozo : Nous avons évoqué deux principes, et je me demande si vous pourriez nous en dire un peu plus à leur sujet. Le premier est celui de la nécessité de la proportionnalité. Dans quelle mesure cette notion est-elle subjective? Le projet de loi est-il suffisamment précis sur ce point, ou ce principe sera-t-il affiné au fil de la jurisprudence ou des décisions judiciaires?

M. Noël : Pour répondre à votre première question, il s'agit de principes de droit. Ils ont été développés par la jurisprudence au fil des siècles. La proportionnalité remonte à la Grèce antique.

Ce n'est pas un nouveau principe. Il est utilisé, sénateur, au quotidien en droit administratif. Un fonctionnaire doit justifier ses décisions. Pour cela, il doit être capable d'analyser les facteurs, même lorsqu'ils sont contradictoires.

Je reviens aux avantages de l'arrêté pour l'administration de la justice, car c'est le propos. Cependant, en même temps, on peut s'interroger sur les effets possibles de l'arrêté sur les personnes auxquelles le fournisseur de services électroniques fournit des services, ou sur la vie privée.

Is the benefit of the order to the administration strong enough to impose itself on a potential impact on the privacy of individuals? There's a balancing. The minister has to justify it. There's a requirement for proportionality. That means the decision may be found to be unreasonable.

[*Translation*]

Senator Dalphond: I have two quick questions for Mr. Noël.

First, if representations are made, will you be getting a copy? Proposed section 8 provides for an opportunity to make representations to the ministers. Will you receive these as well?

Mr. Noël: Yes.

Senator Dalphond: Second, since proposed subsection 7(3) sets out a number of factors in a non-exhaustive list, is the principle of proportionality not already implicit in those criteria, which may at times be in tension with one another, such that, even if it were not added to the bill, a decision-maker such as yourself would still have to apply it?

Mr. Noël: I recognize the appeal court judge in that question. I can tell you that the answer is yes, it is implicit. That is the position we took before the House of Commons committee. As both the Privacy Commissioner of Canada and I have said, including it serves to ensure that the minister understands that decisions must be justified on the basis of proportionality and necessity. It imposes an obligation, Senator Dalphond, to such an extent that, if it is not there, the minister's decision could be found to be unreasonable.

I can tell you that I have found a number of decisions to be unreasonable. Indeed, the legislation did not authorize the activity that was being proposed. That has happened before, and the system works. It is a kind of insurance policy. That is how I see it.

Senator Dalphond: And you have the representations?

Mr. Noël: Yes.

Senator Dalphond: Thank you.

Senator Martel: My question is for both Mr. Dufresne and Mr. Noël.

I'd like to return to the necessity and proportionality test. In the absence of such a test in the legislation, what consequences could arise if a requirement imposed on a service provider were challenged before the courts?

Mr. Dufresne: I believe that adding the necessity and proportionality test would certainly strengthen the case against any judicial challenge that might arise, as it would demonstrate

Les avantages de l'arrêté pour l'administration de la justice sont-ils suffisamment importants pour l'emporter sur les effets possibles sur la vie privée des gens? C'est une question d'équilibre. Le ministre doit justifier sa décision. Il y a une exigence de proportionnalité. Cela signifie que la décision pourrait être jugée déraisonnable.

[*Français*]

Le sénateur Dalphond : J'ai deux petites questions pour M. Noël.

Premièrement, si des observations ont été faites, en recevez-vous une copie? L'article 8 permet de faire des observations aux ministres. Allez-vous les recevoir?

M. Noël : Oui.

Le sénateur Dalphond : Deuxièmement, puisque le paragraphe 7(3) prévoit différentes choses qui ne sont pas une liste limitative, au fond, est-ce que le principe de la proportionnalité n'est pas implicite à la lecture des critères qui sont contradictoires et, par conséquent, même si l'on ne l'ajoutait pas à la loi, le décideur que vous êtes devrait l'appliquer?

M. Noël : J'entends le juge de la Cour d'appel qui pose une question. Je peux vous dire que oui, c'est implicite. C'est la réponse que nous avons dite au comité de la Chambre des communes. Comme le commissaire à la protection de la vie privée du Canada et moi-même disons, dans le but de s'assurer que le ministre sait qu'il doit justifier par proportionnalité et nécessité, cela impose une obligation, sénateur Dalphond, à tel point que si ce n'est pas là, à ce moment-là, sa décision pourrait être déclarée non raisonnable.

Je dois vous dire que j'ai déclaré non raisonnables plusieurs décisions. En effet, la législation ne prévoyait pas l'activité qui souhaitait être faite. Cela a déjà eu lieu et cela fonctionne. C'est un genre de police d'assurance. C'est ainsi que je le vois.

Le sénateur Dalphond : Les observations, vous les avez?

M. Noël : Oui.

Le sénateur Dalphond : Merci.

Le sénateur Martel : Ma question est pour Me Dufresne et M. Noël.

J'aimerais revenir sur le critère de nécessité et de proportionnalité. En l'absence d'un tel critère dans la loi, quelles pourraient être les conséquences d'une obligation imposée à un fournisseur en cas de contestation judiciaire?

Me Dufresne : Je crois que l'ajout des critères de nécessité et de proportionnalité renforcera certainement l'action face à toute contestation judiciaire qui pourrait venir, car cela démontrerait

that Parliament required, and that the minister in fact considered, those factors. It would ensure that the order is, both in substance and in appearance, more narrowly tailored, since the minister would be required to demonstrate why it is truly necessary and that the impacts on privacy have been minimized. I believe that would have a very beneficial effect.

Senator Martel: Mr. Noël, do you have anything to add?

Mr. Noël: It is important to understand that, in this process, the provider has an opportunity to be heard. The provider is aware of the order that the minister intends to issue and is therefore in a position to assess whether the minister is complying with the obligations imposed on him or her. The service provider can present its views. At that point, of course, the commissioner, having the benefit of the file and the various perspectives before him, is in a position to make an informed decision.

Senator Martel: Thank you.

[*English*]

Senator Patterson: I am sorry to put you in the hot seat, Intelligence Commissioner. We've received many letters from Canadians across the country with concerns.

One of the letters I received was from a group of academics at the University of Waterloo. What they were talking about is that the legislation itself, when it comes to bills and orders, seems to tilt in the direction of the government.

One of the points they brought forward is the fact that there's no similar procedure for providers to challenge a regulation or order. While you must give the approval before a regulation or order goes forward, it is based on the reasonableness of the minister's conclusion. There is no requirement in the legislation to consult independent technical expertise.

Can you talk about this, please, and what the process will look like for clarity purposes?

Mr. Noël: Thank you for the question. The point of view of the service provider will be part of the record. However, keep in mind that the service provider has its own interests. It may have the interests that we're seeing here in the factors to consider, but there may be other interests. The commissioner is not a part of that. He or she will be looking at the issues. We'll have different points of view.

I sympathize with academics who are imagining things that are sometimes worse than nature, and I say that respectfully. It is true there has to be proper supervision of police and intelligence matters by NSIRA.

que le législateur a demandé et le ministre a, dans les faits, considéré ces facteurs. Cela fait en sorte que l'ordonnance sera, en réalité et en perception, plus ciblée, car il aura eu l'obligation de démontrer pourquoi on en a vraiment besoin, et qu'on a minimisé les impacts sur la vie privée. Je crois que cela aura un effet très bénéfique.

Le sénateur Martel : Monsieur Noël, avez-vous des éléments à ajouter?

M. Noël : Il est important de réaliser que, dans ce processus, le fournisseur a l'occasion de se faire entendre. Il connaît l'ordonnance que le ministre entend émettre et, à ce moment-là, le fournisseur de services est capable de voir l'obligation que le ministre a. Est-ce qu'il se conforme? Il est capable de présenter son point de vue. Évidemment, à ce moment-là, le commissaire qui a le dossier et les différents points de vue est capable de prendre une décision éclairée.

Le sénateur Martel : Merci.

[*Traduction*]

La sénatrice Patterson : Je suis désolée de vous mettre sur la sellette, monsieur le commissaire au renseignement. Nous avons reçu de nombreuses lettres de Canadiens de partout au pays exprimant leurs préoccupations.

L'une des lettres que j'ai reçues venait d'un groupe d'universitaires de l'Université de Waterloo. Selon eux, la loi elle-même — en ce qui concerne les projets de loi et les arrêtés — semble pencher en faveur du gouvernement.

Ils mentionnent notamment l'absence d'une procédure semblable permettant aux fournisseurs de services de contester un règlement ou un arrêté. C'est vous qui devez approuver préalablement un règlement ou un arrêté, mais cette approbation repose sur le caractère raisonnable de la conclusion du ministre. La loi n'exige pas la consultation d'experts techniques indépendants.

Pour que les choses soient claires, pouvez-vous développer ce point et expliquer à quoi ressemblera le processus?

M. Noël : Je vous remercie de cette question. Le point de vue du fournisseur de services figurera dans le compte rendu. Cependant, il faut garder à l'esprit qu'il a ses propres intérêts. Il peut avoir ceux dont nous parlons ici, parmi les facteurs à prendre en compte, mais il peut en avoir d'autres. Le commissaire n'a aucun intérêt dans tout cela. Il examine les enjeux. Il y aura différents points de vue.

Je comprends que des universitaires imaginent parfois des scénarios pires que la réalité, et je dis cela avec tout le respect qui leur est dû. Il est vrai que l'OSSNR doit assurer une surveillance adéquate des activités de police et de renseignement.

At the same time, reality must prevail. The benefit to Canadians must be evaluated. I perceive the role of the commissioner as being right in the middle. The service provider may have, for its own purposes, the privacy of Canadians in mind, but the real decision maker at the end is not the service provider, nor the minister. The decision has to be reasonable.

Senator Dhillon: Commissioner Dufresne, you had in your recommendations that the new subscriber information production order be limited to telecommunication service providers.

One of the challenges we face in law enforcement today is that criminal activity is no longer confined to traditional telecommunication networks. Individuals involved in organized crime, extortion and other serious offences increasingly rely on a variety of digital services to conceal their identities and activities.

If Parliament were to adopt your recommendation, how would investigators obtain subscriber information from services that fall outside of that definition, particularly where identifying the individual behind an account is a first step in an investigation?

Have you considered whether this restriction could create investigative gaps the legislation is specifically intending to address?

Mr. Dufresne: The short answer is the police authorities would be able to get that through the general production order under the Criminal Code. It would be at a higher standard of reasonable belief.

In my view, the powers that would be granted under Bill C-22 would still be more than what the police currently have. It would expand on what they can now do in terms of the reasonable suspicion criterion.

The fine balance has to be some powers where the police officer on their own can get it, some where they go to a judge on reasonable suspicion and some where they go to a judge on reasonable beliefs.

My recommendation is to ensure you're not expanding the category too much where reasonable suspicion alone is going to be enough to obtain the production order.

En même temps, il faut être réaliste. Nous devons évaluer les avantages pour les Canadiens. Je considère que le rôle du commissaire se situe exactement à mi-chemin. Le fournisseur de services peut s'intéresser, pour ses propres fins, à la protection de la vie privée des Canadiens, mais au final, le véritable décideur n'est ni le fournisseur de services ni le ministre. La décision doit être raisonnable.

Le sénateur Dhillon : Monsieur le commissaire Dufresne, vous avez indiqué dans vos recommandations que la nouvelle ordonnance de communication des renseignements relatifs à l'abonné ne devrait s'appliquer qu'à l'égard des fournisseurs de services de télécommunications.

L'un des défis auxquels nous faisons face aujourd'hui en matière d'application de la loi est que les activités criminelles ne se limitent plus aux réseaux de télécommunications traditionnels. Les personnes impliquées dans le crime organisé, l'extorsion et d'autres infractions graves ont de plus en plus recours à divers services numériques pour dissimuler leur identité et leurs activités.

Si le Parlement adoptait votre recommandation, comment les enquêteurs obtiendraient-ils les renseignements relatifs à l'abonné auprès de services qui ne répondent pas à cette définition, surtout lorsque l'identification de la personne qui se cache derrière un compte constitue la première étape d'une enquête?

Vous êtes-vous demandé si cette restriction pourrait créer des lacunes dans les enquêtes, alors que le projet de loi vise précisément à les combler?

Me Dufresne : En bref, la police pourrait obtenir ces renseignements au moyen de l'ordonnance générale de communication prévue dans le Code criminel. Cela se ferait selon la norme plus stricte des motifs raisonnables de croire.

À mon avis, les pouvoirs accordés en vertu du projet de loi C-22 dépasseraient quand même ceux dont dispose actuellement la police. Ils élargiraient le champ d'action des policiers par rapport à ce qu'ils peuvent faire actuellement en vertu du critère du soupçon raisonnable.

Il faut trouver un juste équilibre : certains pouvoirs permettraient aux policiers d'obtenir les renseignements par eux-mêmes; dans d'autres cas, les policiers devraient passer par un juge en démontrant l'existence de soupçons raisonnables; et dans d'autres cas encore, ils devraient démontrer l'existence de motifs raisonnables de croire.

Je recommande de ne pas élargir de manière excessive la catégorie dans laquelle un soupçon raisonnable suffirait à lui seul pour obtenir une ordonnance de communication.

Senator Yussuff: This bill fills a gap where we have a hole in the country in law enforcement having to do their responsibility, and that hole is large.

At the same time, there is a fair degree of concern by Canadians — which may be warranted or unwarranted — because of other people inflaming the situation.

The reality is this legislation is, at this stage, hoping to look beyond our current horizons. How do we assure Canadians, writ large, that this is not an overreach by the government on their behalf and that it is also not an overreach that gives the police far more power than they should be entitled to in our legal and constitutional contexts in how they might exercise it?

Mr. Dufresne: In my view, we do that by having definitions that are narrow and by incorporating elements of necessity and proportionality. That stands the test of time. It's not dependent on technology where it is now. If you have fast-moving AI, quantum and all of those things, factors like necessity and proportionality are flexible and are technology neutral.

I have made some other recommendations. If there are genuine concerns and there's a need for independent assessment, there are ways of doing that. The goal should be avoiding a zero-sum game, making sure we're protecting the fundamental rights of Canadians but making sure the police have the tools they need to do their critical work.

The Chair: Thank you so much.

This brings us to the end of our rapid hour and our time with this panel. Thank you so much for your concise and explicit responses.

We plan, but I think you've set the table really well for the next hour for our colleagues. I want to thank you deeply for that.

For this next hour, we have the honour of welcoming the Honourable Gary Anandasangaree, Minister of Public Safety, and the Honourable Sean Fraser, Minister of Justice and Attorney General of Canada.

Welcome, ministers.

Minister Anandasangaree, I understand you are joined by Vanessa Lloyd, Senior Deputy Director, Policy and Strategic Partnerships, Canadian Security Intelligence Service; Richard Bilodeau, Assistant Deputy Minister, National and Cyber Security Branch, Public Safety Canada; and Marie-Claude

Le sénateur Yussuff : Ce projet de loi comble une lacune importante dans le cadre de l'application de la loi au pays, qui empêche les forces de l'ordre d'agir.

Parallèlement, les Canadiens expriment certaines inquiétudes — justifiées ou non — parce que d'autres personnes enveniment la situation.

En réalité, ce projet de loi vise, à ce stade, à voir plus loin que nos horizons actuels. Comment pouvons-nous garantir à l'ensemble des Canadiens qu'il ne s'agit pas d'un abus de pouvoir de la part du gouvernement à leur égard, ni d'un abus qui accorderait à la police beaucoup plus de pouvoirs qu'elle ne devrait en avoir — compte tenu de nos cadres juridiques et constitutionnels — quant à la manière dont elle pourrait exercer ces pouvoirs?

Me Dufresne : À mon avis, nous pouvons y parvenir en adoptant des définitions strictes et en intégrant les principes de nécessité et de proportionnalité. Ces principes résistent à l'épreuve du temps. Cela ne dépend pas de l'état actuel de la technologie. Face à une IA qui évolue à toute vitesse, à l'informatique quantique et à toutes ces choses, des facteurs comme la nécessité et la proportionnalité sont souples et neutres sur le plan technologique.

J'ai formulé d'autres recommandations. S'il existe des préoccupations légitimes et qu'une évaluation indépendante s'impose, il est possible de l'obtenir. L'objectif devrait être d'éviter un jeu à somme nulle, en veillant à ce que les droits fondamentaux des Canadiens soient protégés, tout en garantissant que la police dispose des outils dont elle a besoin pour mener à bien son travail essentiel.

La présidente : Merci beaucoup.

Ainsi se termine cette heure qui est passée en un éclair avec ce groupe de témoins. Merci beaucoup pour vos réponses concises et claires.

Nous planifions, mais je pense que vous avez très bien préparé le terrain pour l'heure à venir avec nos collègues. Je tiens à vous en remercier sincèrement.

Pour la prochaine heure, nous avons l'honneur d'accueillir l'honorable Gary Anandasangaree, ministre de la Sécurité publique, et l'honorable Sean Fraser, ministre de la Justice et procureur général du Canada.

Bienvenue, messieurs les ministres.

Monsieur le ministre Anandasangaree, je crois comprendre que vous êtes accompagné de Vanessa Lloyd, directrice adjointe principale, Politiques et partenariats stratégiques, Service canadien du renseignement de sécurité; Richard Bilodeau, sous-ministre adjoint, Secteur de la sécurité nationale et de la

Dandenault, Deputy Commissioner, National Specialized Services, Royal Canadian Mounted Police.

Minister Fraser, you are joined by Kimberly Gibner, Deputy Assistant Deputy Minister, Policy Sector, Department of Justice Canada.

That was a mouthful, and it's a roomful. We had a very informative first hour, starting to deep-dive into this bill after much correspondence with Canadians over the past three months. We are very excited to be here and to have you here today.

We invite you to provide opening remarks, to be followed by questions from our members. You have five minutes each.

Hon. Gary Anandasangaree, P.C., M.P., Minister of Public Safety: Thank you, Madam Chair.

At the outset, let me welcome the new members who are here today, Senator Tucker and Senator Martel. It is great to see you both.

Of course, I begin by thanking all of you for your work.

[*Translation*]

Thank you for inviting me to speak to Bill C-22 today.

[*English*]

I would like to acknowledge that we are meeting on the traditional territory of the Algonquin Anishinaabeg people.

I want to also thank Senator Dhillon and his team for his work on this bill. Thank you, senator.

Every day, law enforcement across Canada works to keep our communities safe. They investigate organized crime networks, pursue human traffickers, protect children from online exploitation and respond to cybercriminals who can reach victims from anywhere in the world.

While crime has evolved, our laws and investigative tools have not. Criminals exploit technology. They move quickly across platforms, jurisdictions and borders.

Meanwhile, investigators face delays in obtaining basic information that may be critical to preventing harm, identifying a suspect or rescuing a victim. That is why Bill C-22 matters.

cybersécurité, Sécurité publique Canada; et Marie-Claude Dandenault, sous-commissaire, Services spécialisés nationaux, Gendarmerie royale du Canada.

Monsieur le ministre Fraser, vous êtes accompagné de Kimberly Gibner, sous-ministre adjointe déléguée, Secteur des politiques, ministère de la Justice Canada.

Voilà un groupe de témoins impressionnant, et la salle est comble. Nous avons eu une première heure très instructive par laquelle nous avons entamé notre examen approfondi du projet de loi à la suite d'une vaste consultation auprès des Canadiens au cours des trois derniers mois. Nous sommes très heureux d'être ici et de vous compter parmi nous aujourd'hui.

Nous vous invitons à prononcer votre déclaration préliminaire, qui sera suivie de questions de la part de nos membres. Vous disposez chacun de cinq minutes.

L'hon. Gary Anandasangaree, c.p., député, ministre de la Sécurité publique : Merci, madame la présidente.

Tout d'abord, permettez-moi de souhaiter la bienvenue aux nouveaux membres qui sont ici aujourd'hui, la sénatrice Tucker et le sénateur Martel. Je suis ravi de vous voir tous les deux.

Bien sûr, j'aimerais commencer par vous remercier tous pour votre travail.

[*Français*]

Je vous remercie de m'avoir invité aujourd'hui pour discuter du projet de loi C-22.

[*Traduction*]

Je tiens à souligner que nous nous réunissons sur le territoire traditionnel du peuple algonquin anishinabe.

Je tiens également à remercier le sénateur Dhillon et son équipe de leur travail sur ce projet de loi. Merci, monsieur le sénateur.

Chaque jour, partout au Canada, les forces de l'ordre œuvrent pour assurer la sécurité de nos collectivités. Elles enquêtent sur les réseaux du crime organisé, traquent les trafiquants d'êtres humains, protègent les enfants contre l'exploitation sexuelle en ligne et luttent contre les cybercriminels qui peuvent atteindre leurs victimes de n'importe où dans le monde.

La criminalité a évolué, contrairement à nos lois et à nos outils d'enquête. Les criminels exploitent la technologie. Ils se déplacent rapidement d'une plateforme à l'autre, d'un endroit à l'autre et font fi des frontières.

Pendant ce temps, nos enquêteurs se heurtent à des retards dans l'obtention de renseignements de base qui peuvent s'avérer essentiels pour prévenir un préjudice, identifier un suspect ou

This bill is about ensuring that when a judge authorizes an investigation, law enforcement has the ability to carry out that authorization. It establishes a modern, lawful access framework, one that will protect victims and equip law enforcement with the modern tools they need.

The legislation before you today was shaped by significant engagement with stakeholders and parliamentarians. That collaboration did not weaken the bill; it made it stronger.

You will recall we had Bill C-2 which had a lawful access regime similar to this. Over time, we heard Canadians and came back with Bill C-22. Again, based on feedback from committee, we amended the bill significantly at the committee stage in Parliament.

Canadians expect everyone, including big tech and the private sector, to help keep our communities safe. These companies must be active partners in stopping serious crime and protecting Canadians.

The central challenge before us is straightforward: How do we protect both public safety and privacy in an increasingly digital world? Our answer is that public safety and privacy are not in competition. They are complementary objectives, and both are protected in this legislation.

The bill before you ensures that the investigative authorities remain effective while maintaining the legal thresholds, safeguards, oversight and accountability measures that protect Canadians' rights and freedoms. The current legal framework lacks that balance.

Take, for example, a child exploitation investigation where a digital account can disappear before police can identify the individual behind it.

Imagine a human trafficking victim whose location depends on digital evidence that is available one day and gone the next. These are not theoretical challenges. These are real-world public safety realities.

Bill C-22 brings us to the 21st century. It will help ensure that investigations can begin with speed and certainty, rather than losing critical time at the early stage navigating gaps in outdated frameworks. It will mean fewer investigations are stalled at the

secourir une victime. C'est pourquoi le projet de loi C-22 est si important.

Ce projet de loi vise à garantir que, lorsqu'un juge autorise une enquête, les forces de l'ordre aient la capacité d'agir. Il établit un cadre d'accès légal moderne, qui protégera les victimes et dotera les forces de l'ordre des outils modernes dont elles ont besoin.

Le projet de loi que vous examinez aujourd'hui est le fruit d'une consultation approfondie auprès des parties prenantes et des parlementaires. Loin d'affaiblir le projet de loi, cette collaboration l'a renforcé.

Vous vous souviendrez que nous avions présenté le projet de loi C-2, qui prévoyait un régime d'accès légal semblable à celui-ci. Au fil du temps, nous avons écouté les Canadiens et sommes revenus avec le projet de loi C-22. Encore une fois, en nous appuyant sur la rétroaction du comité, nous avons apporté des amendements importants au projet de loi lors de l'étape de l'étude en comité au Parlement.

Les Canadiens s'attendent à ce que tout le monde, y compris les géants de la technologie et le secteur privé, contribue à assurer la sécurité de nos collectivités. Ces entreprises doivent être des partenaires actifs dans la lutte contre la grande criminalité et dans la protection des Canadiens.

Notre principal défi est simple : comment protéger à la fois la sécurité publique et la vie privée dans un monde de plus en plus numérique? Notre réponse est que la sécurité publique et la vie privée ne s'opposent pas. Ce sont des objectifs complémentaires, et l'une et l'autre sont protégées par ce projet de loi.

Le projet de loi qui vous est présenté garantit que les autorités chargées des enquêtes peuvent travailler efficacement tout en maintenant les seuils juridiques et les mesures de protection, de surveillance et de responsabilisation qui protègent les droits et libertés des Canadiens. Le cadre juridique actuel ne présente pas cet équilibre.

Prenons, par exemple, une enquête sur l'exploitation sexuelle d'enfants dans laquelle un compte numérique peut disparaître avant que la police puisse identifier la personne qui se cache derrière.

Imaginez une victime de la traite des personnes dont la localisation dépend de preuves numériques qui sont disponibles un jour et qui ont disparu le lendemain. Ce ne sont pas là des problèmes théoriques. Ce sont des réalités concrètes en matière de sécurité publique.

Le projet de loi C-22 nous fait entrer dans le XXI^{e} siècle. Il contribuera à garantir que les enquêtes puissent démarrer rapidement et avec certitude, au lieu de perdre un temps précieux dès le départ en devant composer avec les lacunes de cadres

starting line and provides a clearer legal pathway from digital identifiers to further investigative steps.

Canada remains the only Five Eyes country without a comprehensive lawful access framework, and criminals know this. I was reminded of this in Australia when I met with our Five Eyes partners in August. That is increasingly difficult to justify when criminals operate globally. Our investigators must work seamlessly with international partners.

Madam Chair, let me be equally clear about what this bill is not. Bill C-22 is not about weakening privacy protections. It is not about surveillance. It is not about creating back doors into Canadians' private communications.

The House of Commons committee has adopted amendments, including a safeguard clarifying that electronic service providers cannot be compelled to decrypt end-to-end user-encrypted information that causes a systemic vulnerability.

We reduced metadata retention requirements to six months from our initial one year. In fact, this will be among the shortest periods of retention of any of the Five Eyes partners, significantly shorter than the retention periods of Australia, France and Italy.

Those changes reflect an important principle: Giving investigators the tools they need should never come at the expense of creating new vulnerabilities for Canadians.

Bill C-22 will help investigators follow critical digital evidence before it disappears, identify suspects more quickly, support victims sooner and prevent harm before it escalates. It will help Canada work more effectively with international partners to pursue justice and support victims.

Ultimately, this bill is about ensuring that our laws reflect the realities of today's world we all live in. Canadians expect us to keep them safe.

I will conclude, Madam Chair. I wish to thank all of you for your hard work on this bill. I especially wish to acknowledge my colleague the Honourable Sean Fraser for his collaboration.

I look forward to your questions and comments.

The Chair: Thank you, minister.

obsolètes. Il réduira le nombre d'enquêtes bloquées d'entrée de jeu et offrira une voie d'accès juridique plus claire, qui permettra de passer aux autres étapes de l'enquête à partir des identifiants numériques.

Le Canada demeure le seul pays du Groupe des cinq à ne pas disposer d'un cadre complet d'accès légal, et les criminels le savent. Je m'en suis rendu compte en Australie lorsque j'ai rencontré nos partenaires du Groupe des cinq en août. Cela devient de plus en plus difficile à justifier, alors que les criminels opèrent à l'échelle mondiale. Nos enquêteurs doivent pouvoir collaborer harmonieusement avec leurs partenaires internationaux.

Madame la présidente, permettez-moi d'être tout aussi clair sur ce que le projet de loi n'est pas. Le projet de loi C-22 ne vise pas à affaiblir les mesures de protection de la vie privée. Il ne s'agit pas de surveillance. Il ne s'agit pas non plus d'ouvrir des portes dérobées dans les communications privées des Canadiens.

Le comité de la Chambre des communes a adopté des amendements, notamment une mesure de protection précisant que les fournisseurs de services électroniques ne peuvent pas être contraints de déchiffrer des renseignements chiffrés de bout en bout par les utilisateurs finaux, si cela crée une vulnérabilité systémique.

Nous avons ramené la période de conservation des métadonnées à six mois, contre un an initialement. En fait, ce sera l'une des périodes de conservation les plus courtes parmi tous les partenaires du Groupe des cinq, nettement inférieure à celles de l'Australie, de la France et de l'Italie.

Ces changements reflètent un principe important : donner aux enquêteurs les outils dont ils ont besoin ne doit jamais se faire au prix de la création de nouvelles vulnérabilités pour les Canadiens.

Le projet de loi C-22 aidera les enquêteurs à suivre les preuves numériques cruciales avant qu'elles ne disparaissent, à identifier plus rapidement les suspects, à venir en aide plus tôt aux victimes et à prévenir les préjudices avant qu'ils ne s'aggravent. Il aidera le Canada à collaborer plus efficacement avec ses partenaires internationaux pour faire respecter la justice et soutenir les victimes.

Au fond, ce projet de loi vise à garantir que nos lois reflètent les réalités du monde d'aujourd'hui. Les Canadiens attendent de nous que nous assurions leur sécurité.

Je vais conclure, madame la présidente. Je tiens à vous remercier tous pour votre travail assidu sur ce projet de loi. Je tiens tout particulièrement à remercier mon collègue, l'honorable Sean Fraser, de sa collaboration.

J'attends avec impatience vos questions et vos observations.

La présidente : Merci, monsieur le ministre.

Now we will hear from Minister Fraser.

[*Translation*]

The Honourable Sean Fraser, P.C., M.P., Minister of Justice and Attorney General of Canada: Thank you, Madam Chair.

Before I begin, I'd like to congratulate the newly appointed senators, especially Senator Martel.

It is a pleasure to see you here instead of on the other side, in the House of Commons.

[*English*]

For no reason whatsoever.

[*Translation*]

As senators are well aware, our public safety strategy rests on three pillars. First, to strengthen the Criminal Code, we are advancing Bills C-14, C-9 and C-16. The second pillar, which is particularly relevant to today's discussion, involves supporting law enforcement and other front-line workers that protect our communities. As an aside, the third pillar concerns investments in long-term community safety.

[*English*]

It is the second pillar I wish to focus on today.

When we talk about supporting those on the front line, we often default to a conversation about how much we're putting toward new officers on the ground. Certainly, that's a part of the conversation, but that's not the whole conversation.

It's important we actually equip those we're asking to keep communities safe with the tools they need to do the job we have asked them to. There are members of this committee who would know well the importance of having the tools to do the job when it comes to public safety.

Specifically, what has alarmed me over the course of conversations I've had in developing this legislation from the early days — and I wish to thank Gary for the leadership role that he's played — is the fact that Canada has gone through the majority of my life without tools that have been available to most of the rest of the world.

We're living in an era when crime is of an increasingly fast-moving, transnational nature, and digital by default. Even with crimes committed in an analog way with real consequences for real people in real communities, the digital footprint can often

Nous allons maintenant entendre le ministre Fraser.

[*Français*]

L'honorable Sean Fraser, c.p., député, ministre de la Justice et procureur général du Canada : Merci, madame la présidente.

Avant de commencer, j'aimerais offrir mes félicitations aux nouveaux sénateurs et aux nouvelles sénatrices, en particulier à Richard Martel.

C'est un plaisir de vous voir ici et non de l'autre côté, à la Chambre des communes.

[*Traduction*]

Sans aucune raison particulière.

[*Français*]

Comme les sénateurs et les sénatrices le savent très bien, nous avons une stratégie pour promouvoir la sécurité publique qui comprend trois piliers. D'abord, et pour renforcer le Code criminel, nous avançons dans les projets de loi C-14, C-9 et C-16. Le deuxième pilier est très important pour la conversation d'aujourd'hui et pour soutenir les policiers et les personnes qui travaillent sur le terrain pour protéger nos communautés. Pour votre intérêt, le troisième pilier a trait aux investissements pour prévenir les crimes à long terme.

[*Traduction*]

C'est sur ce deuxième pilier que je souhaite me concentrer aujourd'hui.

Lorsque nous parlons de soutenir ceux qui sont en première ligne, nous en venons souvent par défaut à discuter des sommes que nous consacrons au recrutement de nouveaux agents sur le terrain. Certes, cela fait partie du débat, mais ce n'est pas tout.

Il est important que nous dotions réellement ceux à qui nous demandons d'assurer la sécurité des collectivités des outils dont ils ont besoin pour accomplir la tâche que nous leur confions. Certains membres de ce comité savent à quel point il est important de disposer des outils nécessaires pour faire son travail en matière de sécurité publique.

Plus précisément, ce qui m'a alarmé au cours des discussions que j'ai eues dès les débuts de l'élaboration de ce projet de loi — et je tiens à remercier M. Anandasangaree pour le rôle de chef de file qu'il a joué —, c'est le fait que, pendant la majeure partie de ma vie, le Canada était dépourvu des outils dont disposent la plupart des autres pays du monde.

Nous vivons à une époque où la criminalité revêt un caractère de plus en plus dynamique, transnational et, par défaut, numérique. Même lorsque des crimes sont commis de manière « analogique », avec des conséquences concrètes pour de vraies

allow us to investigate crime with a view to both preventing it and prosecuting it should the crime take place.

When we're trying to come up with the right strategy, thankfully, we have other leaders in the world we can look to. As the minister mentioned, our Five Eyes partners — and our G7 partners, for that matter — have figured out different ways to address the challenge when it comes to digital evidence as technology advances.

We don't have to reinvent the wheel. We can adopt practices and put protections in place that are unique to the Canadian experience but, nevertheless, will allow law enforcement to do their job more effectively.

Specifically, for my part, I want to focus on Part 1 of the bill, around lawful access, simply empowering law enforcement — when they are investigating a crime — to ask for information about a particular IP address or phone number to say, "Is this on your network?"

When that information is gleaned, after a process plays out contemplated by this legislation, we have created a new ability with the authorization of a judge for law enforcement to seek the court's permission to access subscriber information, to tie an individual to the number or IP address that may be at issue.

Keep in mind that these are not entirely new powers that are impossible in Canada today. However, when you talk to law enforcement, they are time-consuming. When they are dealing with threats that can play out in real time, the need to ensure that we move quickly to prevent crime and not just prosecute it after the harm has fallen upon Canadians could not be more important.

I wish to save as much time as possible for questions, so I'll terminate my comments here. Suffice it to say, I look forward to the questions you may have and the work the Senate will do on this bill to advance public safety in Canada. Thank you.

The Chair: Our witnesses will be with us until 6 p.m. As always, we will do our best to allow time for each member to ask their questions with a brief use of words. Also, officials will be joining us on the next panel, so we can continue some of our questioning then. We have four minutes for each question, including the answer.

The first question will be asked by Senator Cardozo from our steering committee.

personnes au sein de vraies collectivités, l'empreinte numérique nous permet souvent d'enquêter sur ces crimes afin, à la fois, de les empêcher et d'en poursuivre les auteurs en justice, s'ils devaient se produire.

Pour élaborer la bonne stratégie, heureusement, nous pouvons nous inspirer d'autres chefs de file dans le monde. Comme l'a mentionné mon collègue, nos partenaires du Groupe des cinq — et du G7, d'ailleurs — ont trouvé différentes façons de relever le défi lié aux preuves numériques à mesure que la technologie progresse.

Nous n'avons pas à réinventer la roue. Nous pouvons adopter des pratiques et mettre en place des mesures de protection propres à la réalité canadienne, mais qui permettront néanmoins aux forces de l'ordre de faire leur travail plus efficacement.

Plus précisément, pour ma part, je souhaite me concentrer sur la partie 1 du projet de loi, qui porte sur l'accès légal, et qui vise simplement à donner aux forces de l'ordre — lorsqu'elles enquêtent sur un crime — le pouvoir de demander des renseignements sur une adresse IP ou un numéro de téléphone particulier, autrement dit de savoir si cela se passe sur le réseau de tel ou tel fournisseur.

Une fois ces renseignements obtenus, à l'issue d'un processus prévu par le projet de loi, nous avons fait en sorte que les forces de l'ordre puissent demander à un tribunal l'autorisation d'accéder aux renseignements relatifs à l'abonné, afin d'établir un lien entre une personne et le numéro ou l'adresse IP en cause.

Gardez à l'esprit qu'il ne s'agit pas là de pouvoirs entièrement nouveaux qui sont impossibles aujourd'hui au Canada. En fait, les forces de l'ordre nous le disent, ce sont des procédures qui prennent beaucoup de temps. Or, face à une menace en temps réel, il est plus important que jamais de pouvoir agir rapidement pour prévenir le crime, au lieu de simplement poursuivre les auteurs en justice après coup.

Je souhaite consacrer le plus de temps possible aux questions. Je vais donc m'arrêter ici. Inutile de dire que j'ai hâte d'entendre vos questions et de voir le travail que le Sénat accomplira sur ce projet de loi pour renforcer la sécurité publique au Canada. Merci.

La présidente : Nos témoins seront parmi nous jusqu'à 18 heures. Comme toujours, nous ferons de notre mieux pour accorder à chaque membre le temps nécessaire pour poser ses questions en faisant preuve de concision. De plus, des fonctionnaires du ministère se joindront à nous dans le prochain groupe, ce qui nous permettra de continuer de poser nos questions. Nous disposons de quatre minutes par question, réponse comprise.

La première question sera posée par le sénateur Cardozo, membre de notre comité directeur.

Senator Cardozo: Thank you both, ministers, for being here. I appreciate your time. This is an act that has been a long time coming, as you've noted.

Do you think we have the right balance here between lawfully allowing access to information, on the one hand, versus ensuring the privacy of Canadians and the security of end-to-end encryption? We've heard a lot about whether that is in danger.

I raise all of that in the context of Canadian public digital sovereignty.

Do you think it's time for us to consider a public player in the field, such as a Crown corporation, that would play a role in working with platforms and our digital system, which would give us greater assurance in terms of our digital sovereignty?

Mr. Anandasangaree: Let me address the first part of your question.

Sean mentioned that we actually haven't had a proper lawful access framework in almost a generation. The constant inability of law enforcement to be able to access what is, in most countries, easily accessible has, in some cases, threatened the lives of people who might be extorted, sexually exploited and a range of other things where we believe this tool would be exceptionally helpful.

It's important to understand the journey. When Bill C-2 was tabled, I actually talked to many of you around Bill C-2. I received a fair amount of feedback. You will recall that we pulled back and said, in September last year, that we will go back to the drawing board and try to come up with something more in line with our values. That's exactly what we did.

We spoke to a range of stakeholders, including law enforcement, me, Sean and Ruby Sahoda. We essentially went across Canada and spoke to many law enforcement agencies that gave us the specifics of what they were looking for. We then spoke to civil society groups, privacy experts, the Intelligence Commissioner and a range of official government players who have a role in this regulation. Then, we came up with what we believe is the right balance between privacy protection and the ability of law enforcement to do their job with the tools they need.

This was further clarified during the committee process. We were flexible and open to the advice of the committee. For example, the retention of metadata went from one year to six months, which was a critical point because law enforcement had

Le sénateur Cardozo : Je vous remercie tous deux, messieurs les ministres, de votre présence. Je vous suis reconnaissant du temps que vous nous consacrez. Comme vous l'avez souligné, cette loi a mis longtemps à voir le jour.

Pensez-vous que nous ayons trouvé le juste équilibre entre, d'une part, donner un accès légal aux renseignements et, d'autre part, protéger la vie privée des Canadiens et la sécurité du chiffrement de bout en bout? Nombre de témoins se demandent, en effet, si cela est menacé.

Je soulève tout cela dans le contexte de la souveraineté numérique publique du Canada.

Croyez-vous qu'il soit temps pour nous d'envisager de créer une entité publique dans ce domaine, comme une société d'État, qui jouerait un rôle en collaborant avec les plateformes et notre système numérique, ce qui nous donnerait plus d'assurance en matière de souveraineté numérique?

M. Anandasangaree : Permettez-moi de répondre à la première partie de votre question.

M. Fraser a mentionné que nous sommes dépourvus d'un véritable cadre pour l'accès légal aux renseignements depuis près d'une génération. L'incapacité constante des forces de l'ordre à accéder à des données qui, dans la plupart des pays, sont facilement accessibles a, dans certains cas, mis en danger la vie de personnes susceptibles d'être victimes de chantage, d'exploitation sexuelle et d'une série d'autres situations dans lesquelles nous estimons que cet outil serait extrêmement utile.

Il est important de comprendre le chemin parcouru. Lorsque le projet de loi C-2 a été déposé, j'en ai discuté avec bon nombre d'entre vous. J'ai reçu un nombre considérable de rétroactions. Vous vous rappellerez que nous avons fait marche arrière et indiqué, en septembre de l'année dernière, que nous allions repartir de zéro et essayer d'élaborer un projet de loi plus conforme à nos valeurs. C'est exactement ce que nous avons fait.

M. Fraser, Ruby Sahota et moi-même avons consulté tout un éventail de parties prenantes, dont les forces de l'ordre. Nous avons sillonné le Canada pour rencontrer les représentants de nombreux organismes d'application de la loi, qui nous ont expliqué en détail ce qu'ils attendaient exactement. Nous avons ensuite consulté des groupes de la société civile, des experts en protection de la vie privée, le commissaire au renseignement et différents fonctionnaires qui ont un rôle dans cette réglementation. Nous sommes alors parvenus à ce que nous estimons être le juste équilibre entre la protection de la vie privée et la capacité des forces de l'ordre de faire leur travail avec les outils dont elles ont besoin.

Ce point a été précisé davantage au cours des travaux du comité. Nous avons fait preuve de souplesse et nous sommes restés ouverts aux conseils du comité. Par exemple, la période de conservation des métadonnées est passée d'un an à six mois, ce

insisted that it be a year. We went back to law enforcement and asked them to walk us through what a new application looks like. Then, we thought six months might not be ideal, but it does give confidence that, within that timeline, you could do what you need to. If required, there are judicial ways of extending that timeline if you go to court. There was an opportunity for them to do that, but — at the end of the day — the reduction in that timeline was critical.

Then, we had issues around ministerial orders, for example. Who would be the oversight body for that order? That's where the Intelligence Commissioner came in. Any ministerial order will require the consent of the Intelligence Commissioner, who will, regarding a range of issues, assess the validity of that order. If they believe that it is not in line with the law or our protection rights, they have the ability to say no.

Then, we have the three-year review period. Again, that is another important part of the safeguards we have in place.

The Chair: Thank you very much, minister. We appreciate that.

Senator Patterson: Minister Fraser, this one is for you. It picks up on your colleague's comment about the non-criminal side of things. It's about legal authority and the protection of individuals in emergencies.

I will use search and rescue as an example because that is something at the federal level that impacts both the RCMP and the Canadian Armed Forces. One of the challenges is that, in a missing persons case, it does not necessarily involve a criminal act. A person might be lost, injured or experiencing a medical emergency and unable to communicate with family members.

While Bill C-22 addresses access to location information under existing legal authorities, it's important for the people who are watching this to understand whether those authorities sufficiently cover situations where the primary purpose is to protect someone's life. While we talked about human trafficking, it is not necessarily on that side of things.

The Department of Justice's Charter Statement explains that Bill C-22 expands certain exigent circumstance powers to include tracking data, but those powers remain tied to statutory regulatory requirements for exigent circumstances.

qui constituait un point crucial, car les forces de l'ordre avaient insisté pour qu'elle soit d'un an. Nous sommes retournés voir les forces de l'ordre et leur avons demandé de nous expliquer en détail à quoi ressemblerait une nouvelle demande. Nous avons alors estimé que six mois n'étaient peut-être pas la durée idéale, mais que cela donnait l'assurance que, dans ce délai, on pourrait faire le nécessaire. Au besoin, il existe des voies judiciaires pour prolonger cette période en s'adressant à un tribunal. Elles avaient la possibilité de le faire, mais — en fin de compte — la réduction de cette période était essentielle.

Ensuite, nous avions les problèmes concernant les arrêtés ministériels, par exemple. Quelle entité serait chargée de surveiller ces arrêtés? C'est là qu'intervient le commissaire au renseignement. Tout arrêté ministériel devra obtenir l'assentiment du commissaire au renseignement, qui en évaluera la validité à la lumière de différents critères. Si le commissaire estime que l'arrêté n'est pas conforme à la loi ou à nos droits en matière de protection, il a le pouvoir de s'y opposer.

Nous avons également l'examen qui doit être effectué au bout de trois ans. Là encore, il s'agit d'un autre élément important des mesures de protection que nous avons mises en place.

La présidente : Je vous remercie, monsieur le ministre.

La sénatrice Patterson : Monsieur le ministre Fraser, cette question est pour vous. Elle fait suite à l'observation de votre collègue concernant l'aspect non criminel des choses. Elle concerne l'autorité légale et la protection des personnes dans des situations d'urgence.

Je prendrai comme exemple les opérations de recherche et de sauvetage, car il s'agit d'un domaine de compétence fédérale qui touche à la fois la GRC et les Forces armées canadiennes. L'un des défis réside dans le fait que, dans le cas d'une personne disparue, il n'y a pas nécessairement d'acte criminel. Une personne peut s'être égarée, être blessée ou faire face à une urgence médicale et être incapable de communiquer avec sa famille.

Bien que le projet de loi C-22 traite de l'accès aux renseignements de localisation en vertu des pouvoirs légaux existants, il est important que les personnes qui suivent cette discussion sachent si ces pouvoirs couvrent suffisamment les situations dans lesquelles l'objectif premier est de protéger la vie d'une personne. Nous avons parlé de la traite des personnes, mais ce n'est pas nécessairement ce qui se passe ici.

Dans l'Énoncé concernant la Charte qu'il a préparé à propos du projet de loi C-22, le ministère de la Justice explique que ce projet de loi élargit certains pouvoirs liés aux situations d'urgence pour y inclure les données de localisation, mais que ces pouvoirs restent soumis aux exigences réglementaires prévues par la loi dans ces circonstances.

Minister, after that preamble, from a legal perspective, does Bill C-22 provide sufficient authority for police to obtain cellphone location information during an urgent search and rescue operation when there's no reasonable suspicion of criminal activity?

Mr. Fraser: That is a fascinating question. The manner in which I envision the legislation being used, primarily informed from conversations I've had with law enforcement, was about the investigation of a crime rather than an investigation that might be triggered in an emergency that does not involve a crime.

Just for clarity, there are definitions not only in statute but in common law that are considered when exigent circumstances might take place that would allow information to be shared. Typically, you might think of an event of abuse that might be livestreamed or the known whereabouts of a person who might be a subject of human smuggling.

At the risk of pushing the responsibility onto the more talented officials sitting next to me, Ms. Gibner, I am curious about your expectations about the application in a non-criminal emergency situation where the police might still find value in this information.

Kimberly Gibner, Deputy Assistant Deputy Minister, Policy Sector, Department of Justice Canada: The only thing I would add, if it's of assistance, senator, is that the definition of a peace officer or public officer, at least in the Criminal Code, is quite broad, so it does apply in municipal, provincial and all sorts of circumstances, more generally.

Bill C-22, as the ministers have identified, has quite a narrow scope, so it might not apply in the situation you referred to. However, it still applies to public officers and peace officers.

Mr. Fraser: I have one point of follow-up. The reason "exigent circumstances" is defined in the common law is that it can have applications in scenarios that are not necessarily envisioned by Bill C-22. There might be other ways to get such information, but if this is an area where the committee would like to expand the potential applications for emergencies that might not be criminal, I would sincerely welcome the perspectives of the committee in that regard.

Senator Patterson: Thank you.

If use the example of the RCMP and the Canadian Armed Forces during search and rescue in the North or even during an avalanche recovery, people work with their cellphones right now. Again, it's the access to the information. Is the mechanism

Monsieur le ministre, après le préambule, d'un point de vue juridique, le projet de loi C-22 confère-t-il à la police des pouvoirs suffisants pour obtenir des renseignements sur la localisation d'un cellulaire dans une opération urgente de recherche et de sauvetage, lorsqu'il n'existe aucun soupçon raisonnable d'activité criminelle?

M. Fraser : C'est une question fascinante. Dans mon esprit — et je me fonde surtout sur mes conversations avec les forces de l'ordre —, ce projet de loi servirait aux enquêtes sur des crimes plutôt qu'à celles qui pourraient être déclenchées par une situation d'urgence sans lien avec un crime.

Pour préciser les choses, il existe des définitions, tant dans les lois qu'en common law, dont on tient compte pour déterminer si une situation d'urgence permettrait de communiquer des renseignements. On peut penser, par exemple, à des actes de violence qui seraient diffusés en direct ou à une personne dont on connaît la position et qui pourrait être transportée clandestinement par des passeurs.

Au risque de céder la responsabilité aux fonctionnaires plus compétents que moi qui sont assis à mes côtés, madame Gibner, j'aimerais savoir comment vous envisagez l'application du projet de loi dans une situation d'urgence non criminelle où ces renseignements pourraient tout de même être utiles à la police.

Kimberly Gibner, sous-ministre adjointe déléguée, Secteur des politiques, ministère de la Justice Canada : La seule chose que j'ajouterais, si cela peut vous être utile, sénatrice, c'est que la définition d'agent de la paix ou de fonctionnaire public, du moins dans le Code criminel, est assez large. Elle s'applique donc aux contextes municipal et provincial et, plus généralement, à toutes sortes de situations.

Comme les ministres l'ont indiqué, le projet de loi C-22 a une portée assez restreinte, et il pourrait donc ne pas s'appliquer à la situation que vous avez évoquée. Il s'applique toutefois aux fonctionnaires publics et aux agents de la paix.

M. Fraser : J'aimerais ajouter une précision. Si la common law définit les « situations d'urgence », c'est parce que cette notion peut s'appliquer à des cas qui ne sont pas nécessairement envisagés dans le projet de loi C-22. Il existe peut-être d'autres moyens d'obtenir ces renseignements, mais, si le comité souhaite que le projet de loi puisse aussi s'appliquer aux urgences qui pourraient ne pas être de nature criminelle, je serais très heureux de connaître son point de vue à ce sujet.

La sénatrice Patterson : Merci.

Prenons l'exemple de la GRC et des Forces armées canadiennes lors d'opérations de recherche et de sauvetage dans le Nord ou même de recherches après une avalanche. De nos jours, les gens utilisent leur téléphone cellulaire. Encore une fois,

there? There is certainly anecdotal evidence out there that it has made it very difficult to get the information they require.

These are both federal entities that I'm referring to here, which is why I'm asking.

So, should we expressly recognize the protection of human life as a basis for emergency access to location information? Again, it's through the same providers.

Mr. Fraser: Having thought about this in a different context over the past year or so, I want to reserve the ability to ensure there are not any unintended consequences with this new scenario being put to me. It strikes me that it would be a reasonable use of the same information for the purpose of protecting a person who is potentially facing grave danger. I want to ensure there's not some other side of the coin. I don't see it in the moment, but I would certainly undertake to get back to the committee as to how, specifically, we would envision the application in a non-criminal situation that would, nevertheless, get the information.

I expect there are other ways to share information that might not require a court process where you would still be able to have access to it. However, I would be happy to provide follow-up thoughts in writing on this particular question.

Senator Patterson: Thank you. Do I have time just to clarify what I'm looking for?

The Chair: No, you don't; you're way over.

[*Translation*]

Senator Martel: Thank you for being with us today. My question comes from my colleague Senator Claude Carignan, who is not here today.

Minister, Bill C-22 provides certain specific protections for medical information and information protected by solicitor-client privilege. In 2017, Parliament enacted the Journalistic Sources Protection Act to protect the confidentiality of sources in criminal investigations. However, Bill C-22 creates new powers enabling authorities to obtain subscriber information.

Could these new powers allow authorities to identify a journalistic source without having to comply with the protections set out in the Canada Evidence Act and the Criminal Code?

Mr. Fraser: Thank you for the question.

c'est une question d'accès aux renseignements. Le mécanisme existe-t-il? Selon certains témoignages, il est très difficile d'obtenir les renseignements nécessaires.

Je parle ici de deux organismes fédéraux, d'où ma question.

Devrions-nous donc reconnaître expressément que la protection de la vie humaine justifie l'accès d'urgence aux données de localisation? Encore une fois, il s'agit des mêmes fournisseurs.

M. Fraser : J'ai réfléchi à cette question dans un autre contexte au cours de la dernière année environ. Comme vous me présentez une nouvelle situation, je tiens à pouvoir vérifier qu'il n'y aurait pas de conséquences imprévues. À première vue, il serait raisonnable d'utiliser les mêmes renseignements pour protéger une personne qui pourrait courir un grave danger. Je veux m'assurer qu'il n'y a pas un revers à la médaille. Je n'en vois pas pour le moment, mais je m'engage volontiers à préciser au comité comment, selon nous, ce projet de loi pourrait permettre d'obtenir ces renseignements même dans une situation non criminelle.

Je pense qu'il existe d'autres moyens de communiquer ces renseignements qui permettraient d'y avoir accès sans nécessairement passer par les tribunaux. Je serai toutefois heureux de vous faire part par écrit de mes réflexions complémentaires sur cette question.

La sénatrice Patterson : Merci. Ai-je le temps de préciser ce que je cherche à savoir?

La présidente : Non, vous avez déjà largement dépassé le temps qui vous était accordé.

[*Français*]

Le sénateur Martel : Merci d'être avec nous aujourd'hui. La question que je vais vous poser provient de mon collègue, le sénateur Claude Carignan, qui n'est pas ici aujourd'hui.

Monsieur le ministre, le projet de loi C-22 prévoit certaines protections spécifiques pour les renseignements médicaux et les renseignements protégés par le secret professionnel entre l'avocat et son client. En 2017, le Parlement a adopté la Loi sur la protection des sources journalistiques afin de protéger la confidentialité des sources dans les enquêtes criminelles. Cependant, le projet de loi C-22 crée de nouveaux pouvoirs pour les autorités afin d'obtenir des renseignements sur les abonnés.

Ces nouveaux pouvoirs pourraient-ils permettre aux autorités d'identifier une source journalistique sans avoir à respecter les protections prévues par la Loi sur la preuve et le Code criminel?

M. Fraser : Merci de la question.

[*English*]

To be clear, there is a big difference between a confirmation of service demand and subscriber information.

One of the protections I believe is helpful for subscriber information is the requirement that you go before the court to seek judicial authorizations. Generally speaking, I prefer to have a person who is aware of all the facts to understand what's reasonable with the full protections that come from the Charter.

Obviously, when you're dealing with journalists, the right to free expression is paramount. Allowing the judge to understand the circumstances and hear the case would typically be my preference. I'd like them to have the full benefit of the facts with the protections known in the Charter. I believe that they would land in the correct place by protecting journalistic integrity without compromising on public safety.

[*Translation*]

Senator Martel: Mr. Fraser, in its submission to the Standing Committee on Public Safety and National Security, the Canadian Association of Journalists expressed serious concerns about Bill C-22, including the risks it poses to the confidentiality of journalistic sources. What is your response to those concerns? I think it would be a good idea to reassure journalists that the new powers granted under Bill C-22 will not compromise the confidentiality of their sources.

[*English*]

Mr. Fraser: I agree with you on the importance of protecting journalistic sources. Where I think we have a point that we can talk through, now and subsequently, regards whether legislative protection would offer anything that the Charter currently does not. In my view, the Charter offers superior protection to those that would come from the legislation. It is not a question about whether your point is valid. It is about whether the protection is necessary to add incremental value over and above the nature of what's being asked for.

Keep in mind that we're not asking for the content of what people may have shared. We're trying to deal with the identity where there's reasonable suspicion and it is agreed upon by the court that it is reasonable that this information is going to yield value to the investigation. I accept and would demand protection for journalistic sources, but I would question whether adding language to the legislation would be necessary in order to strengthen the protection that already exists under Canadian law.

[*Translation*]

Senator Martel: Thank you.

[*Traduction*]

Pour que les choses soient claires, il y a une grande différence entre un ordre de confirmer la fourniture de services et les renseignements relatifs à l'abonné.

À mon avis, l'une des protections utiles dans le cas des renseignements relatifs à l'abonné est l'obligation de demander une autorisation judiciaire au tribunal. En règle générale, je préfère qu'une personne connaissant tous les faits puisse déterminer ce qui est raisonnable en tenant compte de toutes les protections qu'offre la Charte.

Bien entendu, lorsqu'il s'agit de journalistes, le droit à la liberté d'expression est primordial. Je préfère généralement que le juge puisse prendre connaissance des circonstances et entendre la cause. Je souhaite qu'il dispose de tous les faits et qu'il tienne compte des protections reconnues dans la Charte. Je crois qu'il arriverait à une décision juste, en protégeant l'intégrité journalistique sans compromettre la sécurité publique.

[*Français*]

Le sénateur Martel : Monsieur Fraser, l'Association canadienne des journalistes a exprimé de sérieuses préoccupations concernant le projet de loi C-22 dans sa soumission au Comité permanent de la sécurité publique et nationale, y compris les risques pour la confidentialité des sources journalistiques. Que répondez-vous à ces préoccupations? Il serait pertinent de rassurer les journalistes en leur expliquant que les nouveaux pouvoirs du projet de loi C-22 ne compromettront pas la confidentialité de leurs sources.

[*Traduction*]

M. Fraser : Je suis d'accord avec vous sur l'importance de protéger les sources journalistiques. La question dont nous pouvons discuter, maintenant et par la suite, est de savoir si une protection législative offrirait quelque chose que la Charte n'offre pas déjà. À mon avis, la Charte offre des protections supérieures à celles qu'apporterait la loi. Je ne remets pas en question le bien-fondé de votre propos. Il s'agit de déterminer si, compte tenu de la nature des renseignements demandés, il faut prévoir cette protection pour apporter quelque chose de plus.

Rappelons que nous ne demandons pas le contenu de ce que les gens ont pu communiquer. Nous cherchons à établir leur identité lorsqu'il existe des soupçons raisonnables et que le tribunal juge raisonnable de penser que ces renseignements seront utiles à l'enquête. Je reconnais que les sources journalistiques doivent être protégées, et j'exigerais cette protection. Je me demande toutefois s'il est nécessaire d'ajouter une disposition pour renforcer la protection qui existe déjà en droit canadien.

[*Français*]

Le sénateur Martel : Merci.

[*English*]

Senator Pate: Welcome, ministers. My questions are for both of you. The government has committed, through the Truth and Reconciliation Commission, or TRC, Call to Action 30 and the Missing and Murdered Indigenous Women and Girls Calls for Justice, to eliminate the overrepresentation of Indigenous Peoples. There's also been a similar commitment to eliminate the overrepresentation of Black folks and other racialized people. There have also been concerns raised around politically motivated surveillance in the cases of certain Indigenous leaders.

I'm curious as to what steps the federal government took before introducing Bill C-22 to assess the impacts of its measures — including the expanded investigative powers and lowering of evidentiary thresholds for warrants — on rates of criminalization and incarceration of Indigenous, Black and other marginalized communities, including, in particular, land and water protectors. What are the findings, if there have been any? When can we expect the Gender-based Analysis Plus, or GBA Plus, for this legislation to be tabled? And what's the government's timeline for meeting TRC Call to Action 30?

Mr. Anandasangaree: I'll start with the parts that are directly relevant to this bill. Then, senator, I'd be more than glad to talk more about the work done on our Indigenous and Black justice strategies that are in play right now.

With respect to the surveillance of Indigenous leaders, it is an ongoing conversation. I've had the opportunity to meet with all the national Indigenous organizations. This is with respect to the RCMP in particular. One of the demands they initially imposed was that we release available surveillance information to the individual. As of November 10, we anticipate that Library and Archives Canada will be able to release the available information, and we will share it with both national Indigenous organizations and those who have been impacted.

Coming back to the legislation itself, the entire manner in which lawful access will be implemented is through judicial authorization, save and except for the first element, which is seeking confirmation of service. Beyond that, every element of this will require judicial authorization for Part 1. For issues such as a ministerial order, the oversight is with the Intelligence Commissioner. It is not to repeat the failures of the past, and it has nothing to do with the lawful access regime. The surveillance was motivated by politics and mistrust more than anything else. This is about ensuring that we have Criminal Code and Canada Evidence Act provisions in place for law enforcement to be able to do the type of surveillance that can lead to charges and not just as a fishing expedition.

[*Traduction*]

La sénatrice Pate : Bienvenue, messieurs les ministres. Mes questions s'adressent à vous deux. Le gouvernement s'est engagé, dans le cadre de l'appel à l'action 30 de la Commission de vérité et réconciliation, ou CVR, et des appels à la justice concernant les femmes et les filles autochtones disparues et assassinées, à éliminer la surreprésentation des Autochtones. Il a également pris un engagement semblable à l'égard des personnes noires et des autres personnes racisées. La surveillance de certains dirigeants autochtones pour des motifs politiques a aussi soulevé des préoccupations.

Avant de déposer le projet de loi C-22, quelles mesures le gouvernement fédéral a-t-il prises pour évaluer les effets de ses dispositions — notamment l'élargissement des pouvoirs d'enquête et l'abaissement des seuils de preuve requis pour obtenir un mandat — sur les taux de criminalisation et d'incarcération des Autochtones, des personnes noires et des autres groupes marginalisés, en particulier des défenseurs des terres et de l'eau? Quelles conclusions en a-t-il tirées, le cas échéant? Quand pouvons-nous nous attendre au dépôt de l'analyse comparative entre les sexes plus, ou ACS+, de ce projet de loi? Et dans quel délai le gouvernement prévoit-il de donner suite à l'appel à l'action 30 de la CVR?

M. Anandasangaree : Je commencerai par les éléments qui concernent directement ce projet de loi. Ensuite, sénatrice, je serai très heureux de vous en dire davantage sur le travail accompli dans le cadre de nos stratégies actuelles en matière de justice pour les Autochtones et les personnes noires.

Les discussions se poursuivent au sujet de la surveillance des dirigeants autochtones. J'ai eu l'occasion de rencontrer toutes les organisations autochtones nationales. Il est ici question de la GRC en particulier. L'une de leurs demandes initiales était que nous communiquions à la personne concernée les renseignements de surveillance disponibles. Nous prévoyons qu'à compter du 10 novembre, Bibliothèque et Archives Canada pourra divulguer les renseignements disponibles, et nous les transmettrons aux organisations autochtones nationales ainsi qu'aux personnes touchées.

Pour revenir au projet de loi lui-même, toutes les mesures d'accès légal seront mises en œuvre sur autorisation judiciaire, à l'exception du premier élément, qui consiste à demander confirmation de la fourniture de services. Au-delà de cet élément, tout ce qui relève de la partie 1 nécessitera une autorisation judiciaire. Dans le cas d'un arrêté ministériel, par exemple, le commissaire au renseignement assurera la surveillance. Il ne s'agit pas de répéter les erreurs du passé, lesquelles n'ont rien à voir avec le régime d'accès légal. Cette surveillance était avant tout motivée par des considérations politiques et par la méfiance. Il s'agit de prévoir, dans le Code criminel et la Loi sur la preuve au Canada, des dispositions permettant aux forces de l'ordre d'exercer une surveillance

Senator Pate: When will we see the GBA Plus? Experts have raised concerns about the Charter analysis and whether section 8 actually could be satisfied. Of course, the GBA Plus would inform that as well.

Mr. Fraser: I have read it in full. It exists. We will get it to the committee imminently.

Senator Yussuff: Minister, let me start with the definition of an "electronic service provider" in Bill C-22, which is extraordinarily broad. Toronto is the home of a number of successful VPN companies that provide a service. They have real concerns about whether they could be captured by the legislation. Can you clarify for members of the committee whether VPN providers are considered electronic service providers under this bill?

Mr. Anandasangaree: The term "electronic service provider" is deliberately broad. This is to reflect the speed at which technology is exploding — and that's probably the right word. We know that AI, for example, is going to speed up the growth and the availability of electronic service providers exponentially in a number of ways, so it is deliberately broad. Having said that, the core service providers are telecommunication companies, those who are licensed by the Canadian Radio-television and Telecommunications Commission, satellite companies and social media companies who primarily provide services to the public.

Some VPN providers have expressed concern. I would say two things. First, their concerns have been taken into account. We have put in measures confirming that encryption cannot be compromised. That's a measure that we put in as an amendment as part of the committee process. We've reduced the data retention period from one year to six months, and those are to reflect the concerns of VPN providers.

There are also VPN providers that are deliberately threatening, in some cases, to leave Canada. I've learned from my conversations with Five Eyes partners that the same playbook was used in different countries, including Australia and the U.K. With great respect to companies that provide this service, we value their service, but we also expect them to be good citizens.

When we protect encryption, that means that the end-to-end component of the privacy rights of Canadians is protected because we're protecting end-to-end encryption. At the same time, we are demanding that those who operate in Canada provide law enforcement with the support they need. We're not asking them to break any laws. We're asking them, with judicial

La sénatrice Pate : Quand recevrons-nous l'ACS+? Des experts ont soulevé des préoccupations au sujet de l'analyse fondée sur la Charte et se sont demandé si les exigences de l'article 8 pourraient réellement être respectées. Bien entendu, l'ACS+ éclairerait aussi cette question.

M. Fraser : Je l'ai lue au complet. Elle existe. Nous la transmettrons au comité très bientôt.

Le sénateur Yussuff : Monsieur le ministre, je commencerai par la définition de « fournisseur de services électroniques » dans le projet de loi C-22, qui est extrêmement large. Toronto compte plusieurs entreprises prospères qui offrent des services de réseau privé virtuel, ou RPV. Elles craignent beaucoup d'être visées par le projet de loi. Pouvez-vous préciser aux membres du comité si les fournisseurs de RPV sont considérés comme des fournisseurs de services électroniques au sens du projet de loi?

M. Anandasangaree : La définition de « fournisseur de services électroniques » est volontairement large, pour tenir compte de la vitesse à laquelle la technologie explose — et c'est probablement le mot juste. Nous savons, par exemple, que l'intelligence artificielle va accélérer de façon exponentielle, et de plusieurs façons, la croissance des fournisseurs de services électroniques et de l'offre de leurs services. C'est donc délibéré. Cela dit, les fournisseurs principaux sont les entreprises de télécommunication, celles qui détiennent une licence du Conseil de la radiodiffusion et des télécommunications canadiennes, les entreprises de services par satellite et les entreprises de médias sociaux, qui offrent principalement des services au public.

Certains fournisseurs de RPV ont exprimé des préoccupations. Je dirais deux choses. Premièrement, nous en avons tenu compte. Nous avons prévu des mesures confirmant que le chiffrement ne peut être compromis. C'est une mesure que nous avons ajoutée par amendement lors de l'étude en comité. Nous avons réduit la durée de conservation des données d'un an à six mois. Ces mesures visent à répondre aux préoccupations des fournisseurs de RPV.

Certains fournisseurs de RPV menacent aussi délibérément de quitter le Canada. Mes échanges avec nos partenaires du Groupe des cinq m'ont appris que la même stratégie a été utilisée dans différents pays, dont l'Australie et le Royaume-Uni. Avec tout le respect que je dois aux entreprises qui offrent ce service, nous apprécions leurs services, mais nous attendons aussi d'elles qu'elles se comportent en bons citoyens.

En protégeant le chiffrement de bout en bout, nous protégeons cet aspect du droit des Canadiens à la vie privée. En même temps, nous exigeons que les entreprises qui exercent leurs activités au Canada fournissent aux forces de l'ordre le soutien dont elles ont besoin. Nous ne leur demandons pas d'enfreindre la loi. Nous leur demandons de fournir, sur autorisation

or authorization, to provide information that is authorized by law to be released.

I am of the belief that we have found the right balance, as I've indicated previously. Yes, senator.

Senator Yussuff: But, given that VPN companies are not a primary carrier of this data, they don't store the data. They are only providing a service to stop hackers from getting into your device. It seems that you're saying, on the one hand, they are not the target of this legislation. Is there a better way to clarify that what they do is obviously important and that we value their service, but, at the same time, this legislation is aimed at other actors providing the core services to which law enforcement would ultimately need access?

Mr. Anandasangaree: We made it clear, but we can certainly clarify it further, senator. At the end of the day, our core service providers are telcos. The internet service providers are satellite service providers who provide communication services. The expansion to other platforms is not what is immediately envisioned, although, as technology develops, we want the ability to do that. Again, in some cases, we'll require a ministerial order. If that's the case, then the safeguard is with the Intelligence Commissioner.

Senator Dean: Thanks for joining us. I want to raise the spectre of the so-called back doors in relation to data retention orders. I, for one — and I'm sure I'm not alone — haven't been impressed by service providers' responses, not least because they don't have a particularly good track record of retaining subscriber information within their own boundaries. In fact, we know that some of them sell it. But, further, these organizations have suggested that data retention orders would attract malfeasant actors, and that retained data might then not be secure.

My question and my points are as follows: First, I don't think we're likely to see retention orders published in the *Gazette*. There is the question of how malfeasant actors would find out about these orders. Second, Canadians would expect those companies to assist and work with our security organizations to show them the front door. We know that front doors exist for various reasons.

I have no doubt that the service providers involved in this would work hand in hand with our security organizations to ensure that data is secure. I think Canadians would expect that, too. What's your reaction to that? Mr. Fraser, could I ask you to comment?

judiciaire ou autre, des renseignements dont la communication est autorisée par la loi.

Je crois que nous avons trouvé le juste équilibre, comme je l'ai déjà indiqué. Oui, sénateur.

Le sénateur Yussuff : Mais les fournisseurs de RPV ne sont pas les principaux transporteurs de ces données et ils ne les stockent pas. Ils offrent seulement un service destiné à empêcher les pirates informatiques d'accéder à votre appareil. D'un côté, vous semblez dire qu'ils ne sont pas visés par le projet de loi. Pourrait-on préciser davantage que leurs activités sont évidemment importantes et que nous apprécions leurs services, tout en indiquant que le projet de loi vise d'autres acteurs qui fournissent les services principaux auxquels les forces de l'ordre auraient, au bout du compte, besoin d'accéder?

M. Anandasangaree : Nous l'avons précisé, mais nous pouvons certainement le faire davantage, sénateur. En fin de compte, les fournisseurs principaux sont les entreprises de télécommunication. Les fournisseurs de services Internet sont des fournisseurs de services par satellite qui offrent des services de communication. Nous n'envisageons pas dans l'immédiat d'étendre l'application du projet de loi à d'autres plateformes, mais nous voulons pouvoir le faire à mesure que la technologie évolue. Encore une fois, dans certains cas, il faudra un arrêté ministériel. La protection sera alors assurée par le commissaire au renseignement.

Le sénateur Dean : Merci d'être des nôtres. Je veux soulever la question des fameuses portes dérobées dans le contexte des ordres de conservation des données. Pour ma part — et je suis certain de ne pas être le seul —, les réponses des fournisseurs de services ne m'ont pas impressionné, notamment parce qu'ils n'ont pas un bilan particulièrement reluisant lorsqu'il s'agit de garder les renseignements relatifs aux abonnés au sein de leur propre organisation. Nous savons même que certains les vendent. Ces organisations ont aussi laissé entendre que les ordres de conservation des données attireraient des acteurs malveillants et que la sécurité des données conservées pourrait alors être compromise.

Voici ma question et mes observations : premièrement, il me paraît peu probable que les ordres de conservation soient publiés dans la *Gazette*. On peut donc se demander comment les acteurs malveillants en apprendraient l'existence. Deuxièmement, les Canadiens s'attendraient à ce que ces entreprises aident nos organismes de sécurité et collaborent avec eux pour leur indiquer la porte d'entrée. Nous savons que ces portes existent pour diverses raisons.

Je suis convaincu que les fournisseurs de services concernés travailleraient main dans la main avec nos organismes de sécurité pour garantir la sécurité des données. Je pense que les Canadiens s'y attendraient aussi. Qu'en pensez-vous? Monsieur Fraser, pourriez-vous nous donner votre avis?

Mr. Fraser: One point in your intervention, senator, stuck with me. I will want to save time for Minister Anandasangaree because a lot of the data retention piece falls into his area of responsibility.

Canadians have a fair and reasonable expectation that corporate players would absolutely work with the security apparatus, both to protect the information over which Canadians have a reasonable expectation of privacy but would, at the same time, facilitate the investigative tools that are necessary to help keep our communities safe.

Obviously, a list of examples exists that is as long as my arm, of companies that are custodians of personal information of Canadians that have failed to put protections in place. To the extent that we can work with companies to establish practices to ensure retention of the information that will facilitate the requests under Part 1 of the bill, without compromising on the privacy interests, that is ultimately fair and reasonable. That is not just my own opinion. I think it is a reasonable expectation that most Canadians would have.

Minister Anandasangaree, on the data retention piece, you may have something to supplement that response.

Mr. Anandasangaree: Sure. The safeguard already built in is that anything that would cause systemic vulnerabilities does not need to be implemented. In fact, it is in the interests of the government and law enforcement to ensure there are no backdoor ways in which data can be compromised. It is the responsibility of every electronic service provider to protect their data and protect their systems so that data breaches are avoided at all costs. Those breaches can have significant impacts on Canadians.

The bill enables electronic service providers to protect their data when and if systemic vulnerabilities emerge from those changes. It is their responsibility to continuously assess if, for example, metadata retention would compromise their systems and then to inform us.

Ultimately, senator, it is the responsibility of Canadian business, and we are partners; there's government, there are businesses and there are consumers. Our interest is to support businesses and also to support the safety and security of Canadians. Within this paradigm, we've been able to —

The Chair: Thank you, minister.

Senator Hay: Ministers, thanks for being here. The previous panel suggested they would lob the question back to me to lob it over to you, so you're the lucky recipients.

M. Fraser : Un point de votre intervention m'a marqué, sénateur. Je tiens à laisser du temps au ministre Anandasangaree, car une grande partie du volet sur la conservation des données relève de lui.

Il est juste et raisonnable que les Canadiens s'attendent à ce que les entreprises collaborent pleinement avec l'appareil de sécurité. Il s'agit à la fois de protéger les renseignements à l'égard desquels les Canadiens ont une attente raisonnable en matière de respect de la vie privée et de faciliter le recours aux outils d'enquête nécessaires pour contribuer à la sécurité de nos collectivités.

Bien entendu, la liste des entreprises qui détiennent des renseignements personnels de Canadiens sans avoir mis en place de mesures de protection est longue comme le bras. Dans la mesure où nous pouvons collaborer avec elles pour établir des pratiques qui assurent la conservation des renseignements et facilitent ainsi les demandes prévues à la partie 1 du projet de loi, sans compromettre la protection de la vie privée, cela me paraît tout à fait juste et raisonnable. Ce n'est pas seulement mon avis. Je pense que la plupart des Canadiens s'y attendraient à juste titre.

Monsieur le ministre Anandasangaree, vous avez peut-être quelque chose à ajouter à cette réponse sur la conservation des données.

M. Anandasangaree : Certainement. Une protection est déjà prévue : les mesures qui créeraient des vulnérabilités systémiques n'ont pas à être mises en œuvre. De fait, le gouvernement et les forces de l'ordre ont tout intérêt à ce qu'aucune porte dérobée ne permette de compromettre les données. Chaque fournisseur de services électroniques a la responsabilité de protéger ses données et ses systèmes afin d'éviter à tout prix les atteintes à la sécurité des données. Ces atteintes peuvent avoir de lourdes conséquences pour les Canadiens.

Le projet de loi permet aux fournisseurs de services électroniques de protéger leurs données si ces changements créent des vulnérabilités systémiques. Ils ont la responsabilité de vérifier continuellement si, par exemple, la conservation des métadonnées compromettrait leurs systèmes, puis de nous en informer.

En fin de compte, sénateur, c'est la responsabilité des entreprises canadiennes, et nous sommes des partenaires : le gouvernement, les entreprises et les consommateurs. Nous voulons soutenir les entreprises et assurer la sécurité et la protection des Canadiens. Dans ce cadre, nous avons pu...

La présidente : Merci, monsieur le ministre.

La sénatrice Hay : Messieurs les ministres, merci d'être ici. Les témoins précédents ont proposé de me renvoyer la balle pour que je vous la passe. Vous avez donc la chance d'en hériter.

I really appreciate the intent of the bill in putting 21st-century or even 22nd-century tools into the hands of our law enforcement and public safety. I do want to talk about technology, AI and the warp speed at which they are moving. A three-month cycle is probably slow for technology these days.

When I think of the bill, one could perhaps say it has been built in a different era, which could even be last year, for example. If so, it might not be designed for where we're at right now, which is ever evolving. In particular, we see global risk and global cyber, whether through bad actors or foreign whatnot.

My question for you both is this: How do you see this bill being able to flex and evolve with the speed of technology and risk?

Mr. Fraser: I'm taken back to the day the bill was tabled. Commissioner Carrique, who was also with the Canadian Association of Chiefs of Police, gave one of the most powerful statements in support of this bill's direction that I can recall hearing. He discussed his frustration that it has taken this long to get here, the work having started in the 1990s, when I started Grade 7.

It is remarkable to think of how much time has passed and how much technology has advanced. If you imagine where we may be 30 years from now, we simply can't afford not to have tools to examine the kinds of threats on which we are read in on, literally on a daily basis. Some flexibility needs to be baked into the legislation to allow us to future-proof it against advances in technology that are beyond our current ability to imagine. This includes some flexibility on who will be a service provider because the rate of technological change is so fast that we would be obsolete by the time we achieved Royal Assent.

The Criminal Code seeks to be neutral by design to allow for the application of rules and principles in which we believe to technologies and social phenomena that have not yet come to pass.

My view is that, in a number of ways, the bill seeks to achieve that ability to apply these rules to the technology that exists today that didn't exist in the late 1990s and that have not yet come to exist but which we will certainly see over the next number of years.

Mr. Anandasangaree: I'll add three points. First, we recognize this bill is decades late. It should have been available in the 1990s. I think there were seven attempts to bring the bill

J'apprécie beaucoup l'objectif du projet de loi, qui est de mettre des outils du XXI^{e} ou même du XXII^{e} siècle à la disposition des forces de l'ordre et des responsables de la sécurité publique. Je veux toutefois parler de la technologie, de l'intelligence artificielle et de la vitesse vertigineuse à laquelle elles évoluent. De nos jours, un cycle de trois mois est probablement lent dans le domaine technologique.

Quand je pense à ce projet de loi, je me dis qu'il a peut-être été conçu à une autre époque, même si celle-ci remonte seulement à l'an dernier, par exemple. Si c'est le cas, il n'est peut-être pas adapté à la situation actuelle, qui ne cesse d'évoluer. Je pense notamment aux risques et aux cybermenaces à l'échelle mondiale, qu'ils viennent d'acteurs malveillants, d'acteurs étrangers ou d'autres sources.

Voici ma question à vous deux : comment ce projet de loi pourra-t-il s'adapter et évoluer au rythme de la technologie et des risques?

M. Fraser : Cela me ramène au jour du dépôt du projet de loi. Le commissaire Carrique, qui faisait aussi partie de l'Association canadienne des chefs de police, a appuyé l'orientation de ce projet de loi dans l'une des déclarations les plus marquantes que je me souvienne d'avoir entendues. Il a exprimé sa frustration devant le temps qu'il avait fallu pour en arriver là, alors que le travail avait commencé dans les années 1990, quand j'entrais en septième année.

C'est frappant de voir tout le temps qui s'est écoulé et à quel point la technologie a évolué. Si nous imaginons où nous pourrions en être dans 30 ans, nous ne pouvons tout simplement pas rester sans outils pour examiner les types de menaces dont nous sommes informés littéralement tous les jours. Il faut prévoir une certaine souplesse dans le projet de loi pour qu'il reste pertinent malgré des avancées technologiques que nous ne pouvons pas encore imaginer. Il faut notamment de la souplesse quant aux acteurs qui seront considérés comme des fournisseurs de services, car la technologie évolue si vite que notre cadre serait dépassé avant même la sanction royale.

Le Code criminel se veut neutre dans sa conception, pour que les règles et les principes auxquels nous croyons puissent s'appliquer à des technologies et à des phénomènes sociaux qui n'existent pas encore.

À mon avis, le projet de loi vise, de plusieurs façons, à permettre l'application de ces règles aux technologies d'aujourd'hui, qui n'existaient pas à la fin des années 1990, ainsi qu'à celles qui n'existent pas encore, mais que nous verrons certainement apparaître dans les prochaines années.

M. Anandasangaree : J'ajouterai trois points. Premièrement, nous reconnaissons que ce projet de loi arrive avec des décennies de retard. Nous aurions dû l'avoir dans les années 1990. Je crois

forward. At some point, it should have passed. For whatever reason, it did not, but we're here.

The perspective we've heard from law enforcement is, "Better late than never," but let's also have the agility to evolve. While this will serve as the foundational piece, the built-in three-year review will allow us to have a deliberate review of this bill and to make changes so we're not again starting from scratch.

The ability to address the evolution of technology and electronic service providers is deliberately in there with the ability for us to change and evolve with emerging technology. We don't now have a world in which AI will be able to generate its own electronic service and sell it to Canadians or make it available to Canadians. However, perhaps that is something the regulation and definition could capture.

Similarly, as we look at the ministerial orders, again, it enables expansion. We envision core service providers to be the primary compilers with this. The ability for us to provide ministerial orders that can expand is something that, again, is built in because of the need for that agility.

It is there. It may be imperfect. Critically, it forces us to start somewhere with the ability to evolve over time.

The Chair: Before we ask our next questions, we have four senators left, and I will be razor-sharp with respect to the timing to honour all of you.

Senator Dhillon: I will ask my questions to my colleagues Deputy Commissioner Dandenault and Senior Deputy Director Lloyd.

For Canadians who are watching this today who want to understand what Bill C-22 brings to them when the bill is passed, with what we're struggling with today in law enforcement when we deal with extortion, human trafficking, drugs, fraud, money laundering and all of those things, what are we challenged with today that Bill C-22 will fix for us when this comes into law?

Can you take one case and clarify? For an investigator receiving a complaint today where someone's been defrauded and their life savings have been taken away, or they are being extorted, or you see something online and now they have to act on that, what would that look like?

Marie-Claude Dandenault, Deputy Commissioner, National Specialized Services, Royal Canadian Mounted Police: I will start with Part 1. For me, it is timely access. What

qu'il y a eu sept tentatives de le présenter. À un moment donné, il aurait dû être adopté. Pour une raison ou une autre, ce n'est pas arrivé, mais nous y voici.

Les forces de l'ordre nous ont dit : « Mieux vaut tard que jamais », mais il faut aussi avoir la souplesse nécessaire pour évoluer. Ce projet de loi constituera la base, et l'examen prévu après trois ans nous permettra de l'étudier attentivement et d'y apporter des changements sans devoir repartir de zéro.

Nous avons délibérément prévu la possibilité de tenir compte de l'évolution de la technologie et des fournisseurs de services électroniques, afin de pouvoir nous adapter aux nouvelles technologies. Nous ne vivons pas encore dans un monde où l'intelligence artificielle peut créer son propre service électronique et le vendre aux Canadiens ou le mettre à leur disposition. Toutefois, la réglementation et la définition pourraient peut-être s'appliquer à ce genre de situation.

De même, pour ce qui est des arrêtés ministériels... encore une fois, cela permet une expansion. Nous prévoyons que ces obligations viseront surtout les fournisseurs principaux. Nous avons aussi prévu la possibilité de prendre des arrêtés ministériels qui élargissent cette portée, justement parce qu'il faut cette souplesse.

Cette souplesse est donc prévue. Le projet de loi est peut-être imparfait. Mais, surtout, il nous oblige à commencer quelque part, tout en nous permettant d'évoluer au fil du temps.

La présidente : Avant de passer aux prochaines questions, je précise qu'il reste quatre sénateurs et que je serai très stricte sur le temps de parole, par respect pour vous tous.

Le sénateur Dhillon : Mes questions s'adressent à mes collègues, la sous-commissaire Dandenault et la directrice adjointe principale Lloyd.

Pour les Canadiens qui nous regardent aujourd'hui et qui veulent savoir ce que le projet de loi C-22 leur apportera une fois adopté, pouvez-vous expliquer les difficultés que nous rencontrons actuellement dans les forces de l'ordre face à l'extorsion, à la traite de personnes, aux drogues, à la fraude, au blanchiment d'argent et à tous ces problèmes? Quelles difficultés le projet de loi C-22 résoudra-t-il pour nous lorsqu'il entrera en vigueur?

Pouvez-vous donner un exemple concret? Prenons le cas d'un enquêteur qui reçoit aujourd'hui la plainte d'une personne qui a été victime d'une fraude et qui a perdu les économies de toute une vie, ou qui est victime d'extorsion. Ou encore, il voit quelque chose en ligne et doit intervenir. Comment cela se passerait-il?

Marie-Claude Dandenault, sous-commissaire, Services spécialisés nationaux, Gendarmerie royale du Canada : Je commencerai par la partie 1. Pour moi, l'enjeu est d'avoir accès

I hear most from my teams, and I do have the National Child Exploitation Crime Centre under me, is what they find difficult is when they try to get that first "yes" or "no." Do you provide this service?

I understand Canadians might not understand what that looks like in real time. However, when it takes them days and days, you're adding these days up. If you imagine this might be a child victim, this is continuing to happen. That aspect is frustrating because of the safety of the victim. Sometimes, that is what stands out the most if you're talking about a real case situation. You could talk about a child. There could be another victim of another crime, perhaps an elderly person. While we're not tracking down this suspect doing the crime, they are continuing to act. For me, for Part 1, I can speak on that, for sure.

Vanessa Lloyd, Senior Deputy Director, Policy and Strategic Partnerships, Canadian Security Intelligence Service: I would echo timeliness. Being able to know what network a number or identifier is associated with in a timely manner enables us to consider the next step.

Regarding the subscriber information, ensure you are dealing with the right individual in terms of considering the next step. That might be an intervention with a young person who is being radicalized online. It may be going back to the Federal Court to seek, at a higher legal threshold, intrusive powers to be able to take a more intrusive investigative step.

The range of options available to us to mitigate threats — and to have consistency under Part 2 and know that when you go to ask for those powers necessary to protect Canadians, they are going to be there consistently — will be a game-changer for us to be able to work both domestically and across borders on national security investigations.

Senator Ross: My question is this: How would Bill C-22 affect the sharing of information with foreign entities? What safeguards are in place to ensure that information shared with foreign partners receives protections that are equivalent to those available under Canadian law and the Charter?

Mr. Fraser: There are a number of different ways. I am happy to start. Minister, if you want to supplement, feel free.

This is an issue that operates in two directions. Thankfully, Canada is very experienced in dealing with mutual legal assistance agreements where we share information and evidence to ground investigations and prosecutions, typically governed by treaties we sign with like-minded partners.

aux renseignements en temps opportun. Mes équipes — dont le Centre national contre l'exploitation d'enfants, qui relève de moi — me parlent surtout de la difficulté d'obtenir la première réponse, un « oui » ou un « non », à la question : « Fournissez-vous ce service? »

Je comprends que les Canadiens ne voient peut-être pas ce que cela représente concrètement. Cependant, lorsque cela prend des jours et des jours, les délais s'accumulent. Si la victime est un enfant, imaginez : les actes se poursuivent. C'est frustrant, car la sécurité de la victime est en jeu. Dans un cas réel, c'est parfois ce qui ressort le plus. Il peut s'agir d'un enfant ou d'une autre victime d'un autre crime, peut-être une personne âgée. Tant que nous n'avons pas retrouvé le suspect, il continue de commettre des crimes. Pour ce qui est de la partie 1, je peux certainement en témoigner.

Vanessa Lloyd, directrice adjointe principale, Politique et partenariats stratégiques, Service canadien du renseignement de sécurité : J'insisterais moi aussi sur la rapidité. Savoir en temps opportun à quel réseau un numéro ou un identifiant est associé nous permet d'envisager la prochaine étape.

Les renseignements relatifs à l'abonné nous permettent de vérifier que nous avons affaire à la bonne personne avant d'envisager l'étape suivante. Il pourrait s'agir d'une intervention auprès d'un jeune qui se radicalise en ligne. Ou nous pourrions retourner devant la Cour fédérale pour demander des pouvoirs permettant de prendre une mesure d'enquête plus intrusive. Il faudrait alors répondre à un critère juridique plus exigeant.

Nous disposons d'un éventail de moyens pour atténuer les menaces. La partie 2 apportera aussi de la cohérence. Lorsque nous demanderons les pouvoirs nécessaires pour protéger les Canadiens, nous aurons l'assurance qu'ils seront toujours disponibles. Tout cela changera la donne dans nos enquêtes de sécurité nationale, tant au pays qu'au-delà des frontières.

La sénatrice Ross : Ma question est la suivante : quelle incidence le projet de loi C-22 aurait-il sur la communication de renseignements à des entités étrangères? Quelles garanties sont prévues pour que les renseignements communiqués à des partenaires étrangers bénéficient de protections équivalentes à celles qu'offrent le droit canadien et la Charte?

M. Fraser : Il y a plusieurs façons de procéder. Je veux bien commencer. Monsieur le ministre, n'hésitez pas à compléter ma réponse.

La question se pose dans les deux sens. Heureusement, le Canada a une grande expérience des accords d'entraide juridique qui nous permettent d'échanger des renseignements et des éléments de preuve pour étayer des enquêtes et des poursuites. Ces échanges sont généralement régis par des traités conclus avec des partenaires aux vues similaires.

To make a long story short, when we receive a request from a foreign jurisdiction, we would insist that the protections we're putting in place when Canadian law enforcement is doing an investigation would still be met before we share information with a foreign partner.

Similarly, there's a related issue when Canada is seeking information that may be in the custody of another foreign nation. Something that the process contemplated by this bill provides for is some legitimacy to the request.

Though it may not be required by a supplier of information, it can smooth out the process if you can say, "We actually have a request that's been authorized by Canadian law," though they may not require it, in practice, it has the opportunity to smooth the waters and facilitate the timely sharing of that information to Canada, not just when Canada shares information with a third party.

Senator Ross: Do you have anything to add?

Mr. Anandasangaree: No. All I will say is there are 36 such agreements in place right now, and that could expand over time.

[*Translation*]

Senator Youance: My first question follows up on Senator Hay's question. Parliament is currently being asked to pass Bill C-22. These powers will be used in an ever-changing environment. Is the government open to adding a parliamentary review clause in that regard? Yes or no?

[*English*]

Mr. Anandasangaree: I believe it is there, senator. I believe, typically, it has been five years. I think we deliberately had this reduced to three years.

[*Translation*]

Senator Youance: Do you not think that the five-year period is too long?

[*English*]

Mr. Anandasangaree: That's right. That's why we agreed to a three-year review period.

[*Translation*]

Senator Youance: My second question is for Minister Fraser and has to do with reconciling the objectives of Bill C-22 with the principles established by recent case law.

Pour faire court, lorsque nous recevons une demande de l'étranger, nous exigerions que les protections prévues pour les enquêtes menées par les forces de l'ordre canadiennes soient également respectées avant de communiquer des renseignements à un partenaire étranger.

Une question connexe se pose lorsque le Canada cherche à obtenir des renseignements qui pourraient être détenus par un autre pays. Le processus envisagé dans ce projet de loi confère une certaine légitimité à la demande.

Même si le fournisseur des renseignements ne l'exige pas, le fait de pouvoir dire : « Notre demande a été autorisée en vertu du droit canadien » peut faciliter les démarches. Dans la pratique, cela peut aplanir les difficultés et permettre de communiquer les renseignements au Canada en temps opportun. Cet avantage ne se limite donc pas aux cas où le Canada communique des renseignements à un tiers.

La sénatrice Ross : Avez-vous quelque chose à ajouter?

M. Anandasangaree : Non. Je dirai seulement qu'il existe actuellement 36 accords de ce genre, et que ce nombre pourrait augmenter au fil du temps.

[*Français*]

La sénatrice Youance : Ma première question est à la suite de la question de la sénatrice Hay. Aujourd'hui, le Parlement est appelé à adopter le projet de loi C-22. Ces pouvoirs seront utilisés dans un environnement en constante évolution. Est-ce que le gouvernement est ouvert à l'ajout d'une clause de révision parlementaire touchant ce volet? Oui ou non?

[*Traduction*]

M. Anandasangaree : Je crois que cette disposition y figure, sénatrice. Si je ne me trompe pas, le délai habituel est de cinq ans. Je crois que nous l'avons délibérément ramené à trois ans.

[*Français*]

La sénatrice Youance : Est-ce que la période de cinq ans n'est pas trop longue?

[*Traduction*]

M. Anandasangaree : C'est exact. C'est pourquoi nous avons convenu de prévoir un examen après trois ans.

[*Français*]

La sénatrice Youance : Ma deuxième question s'adresse au ministre Fraser et porte sur la conciliation entre les objectifs du projet de loi C-22 et les principes établis par la jurisprudence récente.

Have there been any court rulings that would limit the application of Bill C-22?

Mr. Fraser: Can I respond in English?

Senator Youance: Yes.

[*English*]

Mr. Fraser: There are a couple more recent Supreme Court decisions that have breathed life into the reasonable expectation of privacy when it comes to the kind of information that has been the subject of a lot of public commentary on this particular bill. I'm thinking of the *Spencer* and *Bykovets* decisions in particular. They build on a long history of principles that can be applied in a modern context that deals with how section 8 of the Charter is interpreted in particular and a long history of practices by law enforcement to investigate crimes for the protection of the public.

I don't know that there is a great reconciliation that needs to take place. We simply need to modernize the application of long-standing principles in a modern and digital context.

There's still going to be a reasonable expectation of privacy that attracts Charter protection under this bill. We very specifically, in order to ensure we're not brushing up against the boundaries of the Charter, have ring-fenced the kind of information that can be the subject of a request that does not require judicial authorization, in particular, knowing whether an account is attached to a particular network, for example.

Second, when we only want basic information that ties a person to the account, we're asking those seeking the information to go before the court.

This is not a common feature of international counterparts who have adopted similar laws. When they are seeking subscriber information, they don't always require judicial authorization.

We're taking it a step further than many of our allies in order to protect privacy, which, in any event, would be protected by the Charter over and above the manner in which it has been ring-fenced for the purpose of this legislation.

Senator Dalphond: Welcome, ministers, to this committee.

When I read the briefs, I found there were concerns expressed about Part 1 over the breadth of the order called the production order. You can have a demand confirmation, which is addressed to a telecom service provider.

Y a-t-il des décisions judiciaires qui ont été prises et qui limitent l'application du projet de loi C-22?

M. Fraser : Est-ce que je peux répondre en anglais?

La sénatrice Youance : Oui.

[*Traduction*]

M. Fraser : Deux arrêts plus récents de la Cour suprême ont donné corps à l'attente raisonnable en matière de respect de la vie privée à l'égard du type de renseignement qui a suscité beaucoup de commentaires publics sur ce projet de loi. Je pense notamment aux arrêts *Spencer* et *Bykovets*. Ils s'appuient sur des principes établis de longue date qui peuvent s'appliquer dans un contexte moderne, notamment pour interpréter l'article 8 de la Charte. Ils s'appuient aussi sur les pratiques que les forces de l'ordre utilisent depuis longtemps pour enquêter sur les crimes afin de protéger le public.

Je ne suis pas certain qu'il y ait grand-chose à concilier. Il faut simplement adapter l'application de principes établis de longue date à un contexte moderne et numérique.

Le projet de loi préservera l'attente raisonnable en matière de respect de la vie privée qui donne droit à la protection de la Charte. Pour nous assurer de ne pas frôler les limites de la Charte, nous avons très précisément circonscrit les types de renseignements qui peuvent faire l'objet d'une demande sans autorisation judiciaire. Il s'agit notamment de savoir si un compte est rattaché à un réseau donné, par exemple.

Deuxièmement, même lorsque nous voulons seulement des renseignements de base qui relient une personne à un compte, nous demandons à ceux qui les cherchent de s'adresser au tribunal.

Ce n'est pas une exigence courante chez nos homologues étrangers qui ont adopté des lois semblables. Lorsqu'ils cherchent à obtenir des renseignements relatifs à l'abonné, ils n'exigent pas toujours d'autorisation judiciaire.

Nous allons plus loin que bon nombre de nos alliés dans la protection de la vie privée, que la Charte protège, dans tous les cas, plus que les mesures avancées dans le projet de loi.

Le sénateur Dalphond : Bienvenue, messieurs les ministres, au comité.

À la lecture des mémoires, j'ai noté des préoccupations concernant la partie 1, plus précisément la portée des ordonnances dites « de communication ». Il est possible dans ce cas d'obtenir la confirmation d'une demande adressée à un fournisseur de services de télécommunications.

But those that express concern, and they are serious — the Privacy Commissioner, the Bar of Quebec and the British Columbia Civil Liberties Association — have written that the definition doesn't refer to an electronic service provider, but a judge may order "a person who provides services to the public" to prepare this information.

They say in the BC Civil Liberties Association:

> Notably, this definition is not specific to electronic service providers, and could be applied to brick-and-mortar service providers like booksellers, daycares, and counselors. . . .

The Bar of Quebec referred to health service systems, including hospitals.

Could you reassure people who have expressed these serious concerns that these are beyond the scope of the bill? Are these things possible?

Mr. Fraser: Let me start by saying that one of the reasons that there is a broader range of service providers who could, in theory, be captured under the subscriber information piece is the fact that we require a court to approve, on the basis of reasonable suspicion, that the information that would be garnered would contribute to the investigation that's being undertaken or the prosecution that would be warranted.

We want it to ensure that we don't simply give access to anyone who asks. However, in addition to having to go through the process where you get information about whether the account is on the network without a warrant, the minute you have identifying information — and a limited amount of information, by the way — we would require a court to approve that.

As I mentioned in response to the last question, this is not a common feature in the international frameworks that have looked at this issue. That additional layer of protection of requiring a court to go to a judge to get basic information about a name and an address attached to the account is a unique Canadian contribution to this conversation on a global basis.

This is not about the information that may be shared, and, in any event, it would have to be approved as reasonable by the court.

In any event, my sense is that the privacy protections that will attach will have a heightened degree of scrutiny as a result of the judicial authorization being required, despite the fact that the

Mais ceux qui expriment des préoccupations — et celles-ci sont sérieuses : le commissaire à la protection de la vie privée, le Barreau du Québec et l'Association des libertés civiles de la Colombie-Britannique — ont fait valoir que la définition ne précise pas un fournisseur de services électroniques et qu'un juge peut ordonner à « une personne qui fournit des services au public » de produire ces renseignements.

Selon l'Association des libertés civiles de la Colombie-Britannique :

> Il convient de noter que cette définition ne se limite pas aux fournisseurs de services électroniques et qu'elle pourrait s'appliquer à des fournisseurs de services traditionnels, comme les librairies, les garderies et les conseillers…

Le Barreau du Québec a fait mention des systèmes de services de santé, y compris les hôpitaux.

Pourriez-vous rassurer les personnes qui ont exprimé ces sérieuses préoccupations en leur confirmant que ces cas ne relèvent pas du champ d'application du projet de loi? De telles situations sont-elles possibles?

M. Fraser : Permettez-moi de préciser : une des raisons pour lesquelles l'éventail des fournisseurs de services susceptibles, en théorie, d'être concernés par la disposition des renseignements sur l'abonné est plus large tient au fait que nous exigeons qu'un juge autorise, sur la base de motifs raisonnable de soupçonner, que les renseignements qui seraient recueillis contribuent à une enquête en cours ou à des poursuites qui seraient justifiées.

Nous voulons ainsi nous assurer de ne pas accorder l'accès à quiconque en fait la demande. Cependant, outre la nécessité de suivre la procédure permettant de vérifier, sans mandat, si le compte figure dans le réseau, dès que des renseignements d'identification deviennent accessibles, des renseignements très limités, soit dit en passant, nous exigerions l'autorisation d'un tribunal.

Comme je l'ai mentionné dans ma réponse à la dernière question, il ne s'agit pas d'une caractéristique courante des cadres internationaux en fonction desquels cette question a été examinée. Ce niveau de protection supplémentaire, qui consiste à exiger que l'on s'adresse à un juge pour obtenir des renseignements de base sur un nom et une adresse associés à un compte, constitue une caractéristique unique au Canada dans ce débat par rapport au reste du monde.

Il ne s'agit pas ici des renseignements qui pourraient être partagés et qui, de toutes les façons, devraient être jugés raisonnables par le tribunal.

Quoi qu'il en soit, j'ai l'impression que les mesures de protection de la vie privée qui s'appliqueront feront l'objet d'un examen plus rigoureux en raison de l'autorisation judiciaire

definition of “service provider” is a little broader for the purpose of that section.

Mr. Anandasangaree: If I may just add, with respect to health and medical information, solicitor-client privilege and, of course, protection of journalists, those are already in case law. As well, Charter protections are embedded for them, and any breach of those will not be in any way part of authorized access through Bill C-22.

Senator Dalphond: Thank you.

The Chair: Thank you all very much.

This brings us to a pre-timed end with our witnesses today.

Thank you, ministers, for taking the time to meet with us, as getting this right really matters. Its relevance today — and the effort of coming back at this over and over — is critical, so thank you, all, for being here.

For this panel, we have the pleasure of welcoming some folks who are returning witnesses, which is fantastic. From Justice Canada, we have Kimberly Gibner, Deputy Assistant Deputy Minister, Policy Sector; and Anne-Marie Lebel, Counsel, Criminal Law Policy Section, Policy Sector. From Public Safety Canada, we welcome Shannon Hiegel, Director General, National and Cyber Security Branch; and Richard Bilodeau, Assistant Deputy Minister, National and Cyber Security Branch. From the Canadian Security Intelligence Service, we have Ramzi Nashef, Director General, Policy, Planning, and Accountability. From the Royal Canadian Mounted Police, we welcome Rick Burchill, Assistant Commissioner; and Sergeant Aaron Gilkes, Acting Officer in-charge, RCMP Lawful Access.

Thank you all, including the support folks who are with you today, for being with us. It is really significant having you around the table together.

We’re going to fly right into questions. We will have our colleagues with us here until 7:00. As always, we will do our best to allow time for each member to ask their questions.

Senator Cardozo: I don’t know who can answer this, but one of the issues that’s come up a lot is breaking the end-to-end encryption. Some people refer to it as a back door. The argument that has been made is that if we allow ESPs to break the end-to-end encryption, we are making the system more vulnerable to the bad guys; whereas, right now, it isn’t broken and, therefore, there is no back door.

requise, même si la définition de « fournisseur de services » est un peu plus large aux fins de cette section.

M. Anandasangaree : Si je peux me permettre d’ajouter, en ce qui concerne les renseignements sanitaires et médicaux, le secret professionnel entre avocat et client et, bien sûr, la protection des journalistes, ces éléments font déjà partie de la jurisprudence. De plus, les protections prévues par la Charte s’y appliquent, et toute violation ne fera en aucun cas partie de l’accès autorisé en vertu du projet de loi C-22.

Le sénateur Dalphond : Merci.

La présidente : Merci beaucoup à tous.

Cela conclut le temps prévu avec nos témoins aujourd’hui.

Merci, messieurs les ministres, d’avoir pris le temps de nous rencontrer, car il est vraiment important de bien faire les choses. La pertinence de cette question aujourd’hui — et l’effort de revenir sans cesse sur ce sujet — est cruciale. Merci à tous d’être venus.

Pour ce prochain groupe, nous avons le plaisir d’accueillir certains témoins qui reviennent, ce qui est formidable. Nous avons le plaisir d’accueillir Kimberly Gibner, sous-ministre adjointe déléguée, Secteur des politiques; et Anne-Marie Lebel, avocate, Section de la politique en matière de droit pénal, du ministère de la Justice du Canada. De Sécurité publique Canada, nous accueillons Shannon Hiegel, directrice générale, Secteur de la sécurité nationale et de la cybersécurité; et Richard Bilodeau, sous-ministre adjoint, Secteur de la sécurité nationale et de la cybersécurité. Du Service canadien du renseignement de sécurité, nous accueillons Ramzi Nashef, directeur général, Politique, planification et responsabilisation. De la Gendarmerie royale du Canada, nous accueillons Rick Burchill, Commissaire adjoint; et le sergent Aaron Gilkes, officier responsable par intérim, Accès légal de la GRC.

Merci à tous, y compris aux personnes qui vous accompagnent aujourd’hui, de votre présence. C’est vraiment important de vous avoir tous réunis autour de cette table.

Nous allons passer directement aux questions. Nos collègues seront parmi nous jusqu’à 19 heures. Comme toujours, nous ferons de notre mieux pour que tous aient le temps de poser leurs questions.

Le sénateur Cardozo : Je ne sais pas qui pourra répondre à cela, mais une des questions qui revient souvent concerne le contournement du chiffrement de bout en bout. Certaines personnes parlent de porte dérobée. L’argument avancé est que si nous permettons aux fournisseurs de services électroniques de contourner le chiffrement de bout en bout, nous rendons le système plus vulnérable aux malfaiteurs; alors qu’à l’heure actuelle, ce chiffrement n’est pas contourné et qu’il n’y a donc pas de porte dérobée.

I would like you to comment on that, please.

Richard Bilodeau, Assistant Deputy Minister, National and Cyber Security Branch, Public Safety Canada: Thank you for that question.

First, one of the amendments that was introduced and passed by the House of Commons was an explicit protection of end-to-end encryption as something that cannot be allowed to be done under this legislation as it now stands. That is one clarification that was made; it sets that out explicitly.

Second, and the minister spoke about this, there is a provision that prevents core providers or electronic service providers that are subject to a ministerial order from instituting, making any or following any order that would put a systemic vulnerability into their system. That could include end-to-end encryption, for example. It could include other changes, but that definition was also clarified to say that a systemic vulnerability is something that is a credible risk as defined against international standards.

Those two specific provisions were put in place in the legislation to address things like end-to-end encryption and ensure that any changes protect systems.

Senator Cardozo: Sergeant Gilkes, I think your role is in regard to lawful access. Can you tell us more about how you deal with that issue now and what you see the bill doing in terms of making things different?

Sergeant Aaron Gilkes, Acting Officer in-charge, RCMP Lawful Access, Royal Canadian Mounted Police: Thank you very much for your question, senator.

For the bill itself, in terms of encryption, it doesn't speak to encryption or decryption. That was actually written in as a clause to purposefully exclude end-to-end encryption.

We currently deal with the same challenges that most law enforcement deals with in terms of encryption. An example would be a banking application. We are all using our banking applications online. We are comfortable that the information is encrypted between us and our bank. However, in the event that police would write, for example, a production order to a bank or financial institution for information in relation to a particular client, they expect to receive that information in an unencrypted format.

There is already an encrypted network that also provides lawful access, with judicial authorization, to police.

J'aimerais que vous commentiez cela, s'il vous plaît.

Richard Bilodeau, sous-ministre adjoint, Secteur de la sécurité nationale et de la cybersécurité, Sécurité publique Canada : Merci pour cette question.

Premièrement, l'un des amendements proposés et adoptés par la Chambre des communes prévoyait une protection explicite du chiffrement de bout en bout, en précisant que le projet de loi, dans sa version actuelle, ne pouvait autoriser cela. Il s'agit là d'une précision qui a été apportée; elle est énoncée explicitement.

Deuxièmement, et le ministre en a parlé, une disposition empêche les fournisseurs de services de base ou les fournisseurs de services électroniques assujettis à un décret ministériel d'instaurer ou de prendre toute mesure qui introduirait une vulnérabilité systémique dans leur système, ou de se conformer à une telle mesure. Ce pourrait être le chiffrement de bout en bout, par exemple. Ce pourrait inclure d'autres modifications, mais on a aussi éclairci cette définition en précisant qu'une vulnérabilité systémique est un risque crédible, selon les normes internationales.

Ces deux dispositions précises ont été intégrées à la loi pour traiter de questions comme le chiffrement de bout en bout et pour garantir que toute modification protège les systèmes.

Le sénateur Cardozo : Sergent Gilkes, je crois que votre rôle concerne l'accès légal. Pouvez-vous nous en dire davantage sur la façon dont vous gérez cette question actuellement et sur ce que, selon vous, le projet de loi changera?

Sergent Aaron Gilkes, officier responsable par intérim, Accès légal de la GRC, Gendarmerie royale du Canada : Je vous remercie de votre question, sénateur.

En ce qui concerne le projet de loi lui-même, celui-ci ne traite ni du chiffrement ni du déchiffrement. Cela a fait l'objet d'une disposition visant, expressément, à exclure le chiffrement de bout en bout.

Nous faisons actuellement face aux mêmes défis que la plupart des forces de l'ordre en matière de chiffrement. Prenons l'exemple d'une application bancaire. Nous utilisons tous nos applications bancaires en ligne. Nous sommes rassurés de savoir que les renseignements entre nous et notre banque sont chiffrés. Toutefois, si la police devait, par exemple, produire une ordonnance de communication à l'intention d'une banque ou d'une institution financière pour obtenir des renseignements concernant un client en particulier, elle s'attendrait à recevoir ces renseignements dans un format non chiffré.

Il existe déjà un réseau chiffré qui permet également à la police d'accéder légalement à ces renseignements, avec une autorisation judiciaire.

Senator Cardozo: So, currently, you do have lawful access to some extent.

Sgt. Gilkes: To some parts of the network, depending on whether the encryption has been provided by the company itself. I'm thinking, for example, of a financial institution, but there are others that can provide that service, depending on how it is currently moving across the network and how that information is stored.

Senator Cardozo: Thank you.

Senator Yussuff: Thank you, witnesses, for being here. I have two questions.

Again, I come back to VPNs. Could you clarify whether a VPN provider that does not currently collect or retain user identification could be required under this legislation to develop the capacity to collect and retain that information? If so, how would that be reconciled with the protections against introducing systemic vulnerabilities — just in that event.

Mr. Bilodeau: Thank you very much for that question.

I think the minister clarified in his remarks to your question, senator, that core providers — the intent is to cover telecommunications, internet service providers and satellite service providers. Others could be the subject of a ministerial order — other electronic service providers — but whether it's through a core provider regulation or through a ministerial order, the legislation, as currently drafted, does not allow for the creation of a systemic vulnerability by applying the different provisions of the legislation.

In certain contexts, it's very fact-specific. Whether it's a VPN or anybody else, if we were contemplating a ministerial order, one of the things the legislation requires us to do is to work with the electronic service provider to understand what the issues are around what we are asking them to do and the feasibility of it, the privacy implications, the cybersecurity implications and cost implications. Justice Noël spoke about that in the first hour. All of those things would need to be taken into account in the making of a ministerial order — and that is in any case, whether it's a VPN or anybody else, for that matter.

Senator Yussuff: This bill has been working its way through Parliament, and we have a short attention span in this country. When something is in front of us, we tend to focus on it, and when it's not there, we kind of do not.

Le sénateur Cardozo : Donc, à l'heure actuelle, vous disposez d'un accès légal dans une certaine mesure.

Sgt Gilkes : À certaines parties du réseau, selon que le chiffrement a été mis en place par l'entreprise elle-même. Je pense, par exemple, à une institution financière, mais d'autres peuvent offrir ce service, selon la façon dont les données circulent actuellement sur le réseau et la manière dont ces renseignements sont stockés.

Le sénateur Cardozo : Merci.

Le sénateur Yussuff : Merci aux témoins d'être ici. J'ai deux questions.

J'en reviens encore une fois aux réseaux privés virtuels, ou RPV. Pourriez-vous préciser si un RPV qui ne recueille ni ne conserve actuellement les données d'identification des utilisateurs pourrait être tenu, en vertu de ce projet de loi, de se doter de la capacité de recueillir et de conserver ces renseignements? Le cas échéant, comment cela s'harmoniserait-il avec les mesures de protection visant à éviter l'introduction de vulnérabilités systémiques — dans ce cas précis seulement?

M. Bilodeau : Merci beaucoup pour cette question.

Je crois que le ministre a précisé dans sa déclaration préliminaire la réponse à votre question, sénateur. Les fournisseurs de services de base — l'intention est de couvrir les télécommunications, les fournisseurs d'accès Internet et les fournisseurs de services par satellite; d'autres pourraient faire l'objet d'un arrêté ministériel, d'autres fournisseurs de services électroniques, mais que ce soit par le truchement d'un règlement sur les fournisseurs de services de base ou d'un arrêté ministériel, le projet de loi, tel qu'il est rédigé actuellement, ne permet pas la création d'une vulnérabilité systémique par l'application de ses différentes dispositions.

Dans certains contextes, cela dépend fortement des faits. Qu'il s'agisse d'un RPV ou de n'importe qui d'autre, si nous envisagions un arrêté ministériel, une des choses que la loi nous oblige à faire est de collaborer avec le fournisseur de services électroniques, pour que soient compris les enjeux liés à ce que nous lui demandons de faire, ainsi que la faisabilité de cette mesure, ses répercussions sur la protection des renseignements personnels, la cybersécurité et les coûts. Le juge Noël en a parlé au cours de la première heure. Tous ces éléments doivent être pris en compte dans la production d'un arrêté ministériel, et ce, dans tous les cas, qu'il s'agisse d'un RPV ou de n'importe qui d'autre.

Le sénateur Yussuff : Ce projet de loi suit son cours au Parlement, et nous avons une capacité d'attention limitée dans ce pays. Lorsqu'une question est à l'ordre du jour, nous avons tendance à nous y concentrer, et, lorsqu'elle ne l'est pas, nous avons tendance à l'oublier.

So, given the vulnerabilities that Canadians have been facing for decades because we haven't had this legislation in place, maybe the RCMP can speak to how this legislation will enhance the responsibility of front-line law enforcement agencies in carrying out their full responsibilities in investigating crimes when they occur, in ways that will bring remedy for those who have been harmed by malicious actors.

Rick Burchill, Assistant Commissioner, Royal Canadian Mounted Police: Thank you for the question, senator.

There are two important streams where this assists law enforcement in Canada. We have talked about them.

One is timely access to information at the very beginning of an investigation. That enhances what we do quite a bit because of the delays associated with some of the barriers that we have now to getting at the front end of an investigation when we know there's been a criminal offence committed and there are victims but we're having trouble getting access to the subscriber information or even the provider of the person who has done the crime. Timely access to that information at the front end will enhance law enforcement significantly.

Then, there is the consistent access to that information.

There are currently service providers in Canada that have the data available when we provide a judicial authorization — they are able to provide it — but that's not all of them. For service providers and law enforcement to have a consistent understanding of what we're capable of getting during a criminal investigation is good for everybody.

[*Translation*]

Senator Martel: Thank you for being here today.

According to the government, how many providers will be considered core providers when the regime is fully implemented?

Mr. Bilodeau: Thank you for the question, senator.

That will depend on who is designated as a core provider. I would not want to say who will be included in that because a regulatory process will follow, but we can look at who is currently providing telecommunications services in Canada: Bell, Telus, Rogers and Vidéotron. I'm sure everyone knows the others. When we look at the list of the top 10, we see a group that covers almost everyone. The same goes for Internet providers, who are often the same players, and satellite service providers. There are not that many companies that provide these services in Canada. The goal is not necessarily to look at the

Ainsi, compte tenu des vulnérabilités auxquelles les Canadiens sont exposés depuis des décennies en raison de l'absence de cette loi, la GRC pourrait peut-être expliquer en quoi celle-ci renforcera la capacité des forces de l'ordre de première ligne à s'acquitter pleinement de leurs responsabilités dans les enquêtes sur les crimes, de sorte qu'ils puissent offrir une réparation aux personnes qui ont été lésées par des acteurs malveillants.

Rick Burchill, Commissaire adjoint, Gendarmerie royale du Canada : Merci pour cette question, sénateur.

Cette loi aide les forces de l'ordre au Canada de deux façons importantes. Nous en avons déjà parlé.

La première est l'accès rapide à l'information dès le tout début d'une enquête. Cela améliore considérablement notre travail, car nous subissons actuellement des retards causés par des obstacles qui nous empêchent d'intervenir dès le début d'une enquête lorsque nous savons qu'une infraction pénale a été commise et qu'il y a des victimes, mais que nous avons de la difficulté à obtenir l'accès aux renseignements sur l'abonné ou même à joindre le fournisseur de services de la personne qui a commis le crime. L'accès rapide à ces renseignements dès le début de l'enquête améliorera considérablement l'efficacité des forces de l'ordre.

Ensuite, il y a la question de l'accès constant à ces renseignements.

Il existe actuellement au Canada des fournisseurs de services qui mettent les données à notre disposition lorsque nous présentons une autorisation judiciaire; ils sont en mesure de les fournir, mais ce n'est pas le cas de tous. Il est dans l'intérêt de tous que les fournisseurs de services et les forces de l'ordre aient une même compréhension de ce que nous pouvons obtenir au cours d'une enquête criminelle.

[*Français*]

Le sénateur Martel : Merci d'être présents aujourd'hui.

Selon le gouvernement, combien de fournisseurs seront considérés comme principaux lorsque le régime sera pleinement mis en œuvre?

M. Bilodeau : Merci de la question, monsieur le sénateur.

Cela dépendra de ceux qui seront définis comme fournisseurs principaux. Je ne voudrais pas dire qui sera inclus, parce qu'un processus réglementaire suivra, mais on peut regarder qui sont les fournisseurs de services de télécommunication au Canada actuellement : Bell, Telus, Rogers, Vidéotron. On connaît les autres. Lorsqu'on regarde la liste des 10 meilleurs, il s'agit d'un groupe qui couvre presque tout le monde. Nous avons la même situation avec les fournisseurs d'Internet — ce sont souvent les mêmes joueurs — et les fournisseurs de services par satellite. Il n'y en a pas énormément qui fournissent ces services au Canada.

number of telecommunications companies but at the coverage they provide.

Senator Martel: Have you conducted a specific analysis on the financial and technical impacts this would have on small and medium-sized providers?

Mr. Bilodeau: That is one of the factors that the minister or the Governor-in-Council has to consider, the financial implications of making these changes. As the assistant commissioner mentioned, various telecommunications service providers already have the capacity to provide the information required, while others do not. That will vary from one provider to another. Discussions will be held with the providers that could be designated as core providers. We expect to discuss that aspect with them before we draft the regulations.

Senator Martel: What empirical analysis led the government to set a retention period of up to six months for certain categories of metadata? Do you have any specific data on the proportion of police requests that involve data dating back at least 30 days, 90 days, six months or longer?

Mr. Bilodeau: I will ask my RCMP colleagues. Their input was used to determine the retention period. As the minister mentioned, it was reduced from one year to six months.

Sgt. Gilkes: Thank you for you question.

It is important to keep in mind that an investigation usually takes several months. We do not usually get all of the information that we need at the beginning of the investigation. We get a lead at the beginning of the investigation and then we have to get legal warrants to get other information, which means that some time may pass before we can get answers from service providers. Then, we need to gather even more information. We need to do more than just identify the IP address. We have to link the device to that IP address and link a user to the device. There are several steps to follow before we can file charges in a criminal investigation.

Senator Martel: Is there no specific time frame? Does it take a fairly long time? Can it take more than a year?

Sgt. Gilkes: Yes, absolutely, depending on the type of investigation. For example, if we are talking about child sexual exploitation, a number of children may have been targeted by the same individual. If all we have is three months' worth of evidence, then we will not be able to identify other potential victims.

Senator Martel: Thank you.

Le but n'est pas nécessairement de regarder le nombre, mais la couverture des fournisseurs de services de télécommunication.

Le sénateur Martel : Avez-vous effectué une analyse particulière sur les conséquences financières et techniques pour les petits et moyens fournisseurs?

M. Bilodeau : C'est un des facteurs que le ministre ou le gouverneur en conseil doit considérer, soit l'implication financière de procéder à ces changements. Tel que le commissaire adjoint l'a mentionné, différents fournisseurs de services de télécommunication ont déjà la capacité de fournir l'information requise et d'autres ne l'ont pas. Cela variera entre fournisseurs. Il y aura des discussions avec les fournisseurs qui pourraient être désignés comme fournisseurs principaux. Avant de faire le règlement, on s'attend à ce que ce soit l'un des aspects de la conversation que nous aurons avec eux.

Le sénateur Martel : Quelle analyse empirique a conduit le gouvernement à retenir une période pouvant aller jusqu'à six mois pour la conservation de certaines catégories de métadonnées? Disposez-vous de données précisant la proportion des demandes policières qui concernent des données datant d'au moins 30 jours, 90 jours, six mois ou plus?

M. Bilodeau : Je vais demander à mes collègues de la GRC. Leur contribution a permis de déterminer la durée de la période. Comme le ministre l'a mentionné, on l'a réduite d'un an à six mois.

Sgt Gilkes : Merci de votre question.

Il faut prendre en considération qu'une enquête dure habituellement plusieurs mois. On ne reçoit généralement pas toutes les informations dont on a besoin au début de l'enquête. On reçoit un indice au début de l'enquête, puis on obtiendra des autorisations judiciaires pour aller chercher d'autres informations, ce qui cause des délais avant d'obtenir des réponses des fournisseurs. Par la suite, il faut encore recueillir d'autres informations. Il faut établir plus que l'adresse IP, il faut associer un appareil avec cette adresse IP ainsi qu'un utilisateur de l'appareil. Il y a plusieurs étapes à suivre avant de pouvoir déposer des accusations dans le cadre d'une enquête criminelle.

Le sénateur Martel : Il n'y a rien de précis au niveau des délais? Cela peut être assez long? Est-ce que cela peut prendre plus d'un an?

Sgt Gilkes : Oui, absolument, dépendamment du type d'enquête. Par exemple, si on parle de l'exploitation sexuelle d'un enfant, il est possible que plusieurs enfants aient été ciblés par un même individu. Si l'on est limité à seulement trois mois de preuve, on ne pourrait pas identifier les autres victimes potentielles.

Le sénateur Martel : Merci.

[*English*]

Senator Pate: My question is probably for you, Ms. Gibner. If not, you can pass it to somebody else.

Extensive evidence, including the work of the MMIWG national inquiry, highlights systemic misogynistic abuse of police powers and even judicial powers to stalk, harass and endanger women, in particular Indigenous women.

I'm curious as to two pieces: First, what measures do you see existing in Bill C-22 to prevent these abuses of power via the new tools that the bill creates? Second, how has the government assessed the risks that additional metadata retention requirement in this bill could create for women whose safety depends on keeping their location and support networks confidential? Who is liable under this bill for harm that it may cause as a result of such breaches?

Ms. Gibner: Thank you very much for the question, Senator Pate. Apologies to the committee who didn't receive the GBA Plus. I understand that it's on its way to you. There was an issue with translation, so you should have it shortly.

The GBA Plus points out the complexity that the Senate is dealing with because, of course, as you quite rightly pointed out, some work is still needed by the criminal justice system as it relates to the issues that you highlighted.

At the same time, the bill really is meant to address assisting law enforcement with detecting those sorts of crimes. You heard our colleagues here talk about some of the child protection issues. Women have the highest numbers with respect to sexual exploitation online.

It really is for this committee to be looking at the GBA Plus that sets out those considerations for you.

Senator Pate: Are you saying the answers to the questions I've just asked about who would be responsible and liable for harm would be in that analysis?

Also, does it address things like the most recent breaches of data, of which we have recently become aware, in Crime Stoppers and in the Alberta voting registry, and the manner in which those breaches put particularly vulnerable women at risk? Are those things addressed in the GBA Plus?

[*Traduction*]

La sénatrice Pate : Ma question s'adresse probablement à vous, madame Gibner. Sinon, vous pouvez la transmettre à quelqu'un d'autre.

De nombreuses preuves, notamment les travaux de l'Enquête nationale sur les femmes et les filles autochtones disparues et assassinées, mettent en évidence une misogynie systémique des pouvoirs policiers, voire judiciaires, traquant, harcelant et mettant en danger les femmes, en particulier les femmes autochtones.

J'aimerais en savoir plus sur deux points. Premièrement, quelles mesures du projet de loi C-22 fourniront de nouveaux outils pour prévenir ces abus de pouvoir? Deuxièmement, comment le gouvernement a-t-il évalué les risques auxquels l'obligation supplémentaire de conserver les métadonnées prévue dans ce projet de loi exposerait les femmes dont la sécurité dépend de la confidentialité de leur localisation et de leurs réseaux de soutien? Qui est responsable, en vertu de ce projet de loi, des préjudices qu'il pourrait causer à la suite de telles violations?

Mme Gibner : Merci beaucoup pour cette question, sénatrice Pate. Toutes nos excuses au comité qui n'a pas reçu l'Analyse comparative entre les sexes, ACS Plus. Je crois comprendre qu'elle est en voie de vous être transmise. Il y a eu un problème de traduction, vous devriez donc la recevoir sous peu.

L'ACS Plus souligne la complexité de la situation à laquelle fait face le Sénat, car, bien sûr, comme vous l'avez très justement souligné, le système de justice pénale a encore du travail à faire en ce qui concerne les enjeux que vous avez mis en évidence.

Parallèlement, le projet de loi vise véritablement à aider les forces de l'ordre à détecter ce genre de crimes. Vous avez entendu nos collègues ici présents aborder certaines questions liées à la protection de l'enfance. Ce sont les femmes qui sont les plus nombreuses à être victimes d'exploitation sexuelle en ligne.

Il est vraiment important que ce comité examiner l'ACS Plus, qui expose ces considérations à votre intention.

La sénatrice Pate : Dites-vous que les réponses aux questions que je viens de poser, soit qui serait responsable et redevable en cas de préjudice, se trouveraient dans cette analyse?

Et traite-t-elle aussi de questions comme les récentes atteintes à la sécurité des données, dont nous avons récemment eu vent, chez Échec au crime et dans le registre électoral de l'Alberta, ainsi que la manière dont ces atteintes à la sécurité mettent en danger des femmes particulièrement vulnérables? Ces questions sont-elles abordées dans l'ACS Plus?

Ms. Gibner: No. The recent incidents that you have talked about are not in the GBA Plus. This is just as it relates to the bill.

Senator Pate: Who is liable for harm caused and how that will be addressed? Is that in the GBA Plus?

Ms. Gibner: No, the GBA Plus is just about the bill and the impact on the different issues that you've talked about. It's just an analysis of that.

Senator Pate: Okay. I ask for this next response in writing. Many concerns were raised about the Charter Statement from legal commentators. It is essentially expanding search and seizure provisions and implicating section 8 of the Charter.

How do you see that being addressed beyond what's in the Charter Statement? I'm out of time, so if you could provide that in writing, that would be great. Thank you.

Senator McNair: Some of you were in the room for the first panel. You heard both the Privacy Commissioner and the Intelligence Commissioner indicating that they would recommend and support amendments to the bill to add the concepts of necessity and proportionality.

My question is first to Ms. Gibner and then to Mr. Bilodeau: Would your respective departments have any objection to that? If so, why?

Ms. Gibner: Thank you very much for the question, senator. I haven't turned my mind to those issues, so I'll pass it over to my colleague, who may have.

Mr. Bilodeau: Thank you, senator, for that question.

As either the Privacy Commissioner or the Intelligence Commissioner noted, we have added an element of "essential" in the retention of metadata. It links back to that.

On proportionality, I would point out that both section 5 and section 7 have a list of factors, whereas we don't use the word "proportionality" in the list. Those factors are all ones that the minister shall or must consider in deciding whether or not to issue a ministerial order or that the Governor-in-Council needs to look at in terms of regulations.

We expect that, in that calculus, all those factors will be considered and weighed in making that decision. Obviously, we

Mme Gibner : Non. Les incidents récents dont vous parlez ne figurent pas dans l'ACS Plus. Celle-ci porte uniquement sur le projet de loi.

La sénatrice Pate : Qui est responsable des préjudices causés et comment cette question sera-t-elle traitée? Est-ce que cela figure dans l'ACS Plus?

Mme Gibner : Non, l'ACS Plus porte uniquement sur le projet de loi et sur son incidence sur les différents enjeux dont vous avez parlé. Il s'agit simplement d'une analyse de ces aspects.

La sénatrice Pate : Bien. Je demande que la réponse suivante me soit fournie par écrit. De nombreuses observations ont été faites par des commentateurs juridiques au sujet de l'énoncé concernant la Charte. Celui-ci élargit essentiellement les dispositions relatives aux perquisitions et aux saisies et touche à l'article 8 de la Charte.

Comment envisagez-vous que cette question soit traitée au-delà de ce qui figure dans l'énoncé concernant la Charte? Je n'ai plus de temps, donc si vous pouviez me fournir cette réponse par écrit, ce serait formidable. Merci.

Le sénateur McNair : Certains d'entre vous étaient présents lors de la première heure de témoignages. Vous avez entendu tant le commissaire à la protection de la vie privée que le commissaire au renseignement indiquer qu'ils recommanderaient et appuieraient des amendements au projet de loi visant à y ajouter les notions de nécessité et de proportionnalité.

Ma question s'adresse d'abord à Mme Gibner, puis à M. Bilodeau : vos ministères respectifs auraient-ils des objections à cela? Le cas échéant, pourquoi?

Mme Gibner : Merci beaucoup pour cette question, sénateur. Je n'ai pas encore réfléchi à ces questions; je vais donc laisser la parole à mon collègue, qui s'est peut-être penché sur le sujet.

M. Bilodeau : Merci, sénateur, pour cette question.

Comme l'ont fait remarquer tant le commissaire à la protection de la vie privée que le commissaire au renseignement, nous avons ajouté une notion « d'essentiel » à la conservation des métadonnées. Cela s'inscrit dans cette optique.

Pour ce qui est de la proportionnalité, je précise que les articles 5 et 7 comportent une liste de facteurs, même si le mot « proportionnalité » n'y figure pas. Ce sont tous des facteurs que le ministre doit prendre en compte pour décider s'il y a lieu de prendre un arrêté ministériel, ou ce que le gouverneur en conseil doit examiner sous l'angle de la réglementation.

Nous nous attendons à ce que, dans ce raisonnement, tous ces facteurs soient pris en compte et pesés lors de la prise de

will take note of the comments from the first hour, analyze them and work internally on that.

Ultimately, it will be up to the committee here and the Senate to decide on that, but we are happy to take a look at that and provide further advice when we have an opportunity to return.

Senator McNair: I realize those factors are there in the legislation, and two commissioners were aware of those. They still felt it was appropriate to ask for the amendment, so I ask you to raise it with your minister.

Mr. Bilodeau: Absolutely.

Senator McNair: Thank you.

[*Translation*]

Senator Youance: I would like to come back to the rapid pace of technological change. What aspects of Bill C-22 are most likely to become obsolete in the short term, given how quickly technology is changing?

Mr. Bilodeau: Thank you for the question.

When drafting Bill C-22, we were fully aware that technology is changing quickly, as we have seen in the past 20 years. The bill, particularly Part 2, is therefore drafted as a legal framework that will be made more specific through regulations and ministerial orders. That will enable us to use the regulations to define certain things, such as electronic service providers. A service may not exist today but could suddenly emerge in two years. If that service were to become people's primary means of communication, then the law would enable us to define it as an electronic service provider.

Senator Youance: In that case, are there any specific safeguards for drafting these regulations?

Mr. Bilodeau: For example, if a new electronic service were to emerge and the government wanted to designate it as a core service provider, that would be done by regulation. We would follow the standard regulatory process, including consultations.

Senator Youance: I have a quick question about systemic vulnerabilities. Are there any mechanisms that enable us to quickly identify whether the implementation of Bill C-22 creates any systemic vulnerabilities? If we find any, what can be done about them?

Mr. Bilodeau: Thank you again for the question.

décision. Évidemment, nous prendrons note des observations formulées au cours de la première heure, nous les analyserons et y travaillerons à l'interne.

En fin de compte, ce sera au comité ici présent et au Sénat de se prononcer à ce sujet, mais nous serons heureux d'examiner la question et de fournir d'autres conseils lorsque nous aurons l'occasion de revenir.

Le sénateur McNair : Je suis conscient que ces facteurs figurent dans le projet de loi et que deux commissaires en avaient connaissance. Ils ont néanmoins jugé opportun de demander cet amendement; je vous demande donc de soumettre la question à votre ministre.

M. Bilodeau : Certainement.

Le sénateur McNair : Merci.

[*Français*]

La sénatrice Youance : J'aimerais revenir sur l'évolution rapide de toute la technologie. Quels éléments du projet de loi C-22 risquent le plus de devenir désuets à court terme, compte tenu de l'évolution rapide des technologies?

M. Bilodeau : Merci de la question.

En rédigeant le projet de loi C-22, nous étions fort conscients que la technologie change rapidement, comme on l'a constaté dans les vingt dernières années. Le projet de loi, surtout la partie 2, est donc rédigé d'une façon où il s'agit d'un cadre législatif qui devra être précisé par des règlements et des ordonnances ministérielles. Cela nous permettra d'utiliser des règlements pour définir des éléments, notamment les fournisseurs de services électroniques. Un service pourrait ne pas exister aujourd'hui et, tout d'un coup, apparaîtra dans deux ans. Si cela devenait le mode de communication principal des gens, la loi nous permettrait de venir les définir comme fournisseurs de services électroniques.

La sénatrice Youance : À ce moment-là, y aurait-il des balises particulières pour la préparation de ces règlements?

M. Bilodeau : Par exemple, un nouveau service électronique fait son apparition et l'on considérait de le désigner comme étant un fournisseur principal, cela se ferait par règlement. On appliquerait donc le processus réglementaire régulier avec des consultations.

La sénatrice Youance : J'ai une petite question sur les vulnérabilités systémiques. Est-ce qu'il y a des mécanismes qui nous permettent de détecter rapidement si l'application du projet de loi C-22 crée des vulnérabilités systémiques? Si l'on en découvre, qu'est-ce qui peut être mis en place?

M. Bilodeau : Merci encore de la question.

I would say that the regulations will be developed through consultation. The best people to tell us whether there are systemic vulnerabilities are the providers themselves because they have an in-depth knowledge of their system. They can tell us whether what we are asking them to do will work or not and whether it will create a vulnerability.

Obviously, on our side, we have experts within the government who helped us with Bill C-22 and who understand these challenges. We can continue to call on them to assist us in developing the regulations and in working with the service providers.

Senator Youance: I would imagine that the implementation of Bill C-22 will involve a lot of information. Do you intend to use AI at the departmental level to analyze that data? Again, what would the safeguards be?

Mr. Bilodeau: It is important to point out that the government will not hold any of that information. The information that could be retained by service providers, the metadata, will not be held by the government. We are not interested in having it. This is people's personal information we are talking about. The only situation where a government entity could access that information would require a search warrant issued by a court and executed by the police. In such cases, there are some safeguards to protect that information.

Senator Youance: Thank you very much.

[*English*]

Senator Dalphond: I have two questions.

[*Translation*]

The first is for Mr. Bilodeau and the second is for Ms. Gibner.

Mr. Bilodeau, you may have heard previous witnesses asking to add the principle of proportionality when it comes to ministerial orders. Would you have a problem with adding that principle and making it more explicit than implicit?

Mr. Bilodeau: If we look at the existing criteria, this principle certainly is implicit. As Mr. Noël mentioned, that is what he would do with the information. We expect, at least implicitly, that this analysis will be conducted. As for whether that principle can be added to the legislation and my minister's position on that, those are discussions that we can have with him. As the process continues, we will have the opportunity to revisit that, or at least I hope we will, and we can discuss it then.

Senator Dalphond: Thank you.

Je vous dirais que l'élaboration des règlements, par exemple, se fera en consultation. Les meilleures personnes pour nous dire s'il y a des vulnérabilités systémiques sont les fournisseurs eux-mêmes, car ils connaissent profondément leur système. Ils peuvent nous dire que ce que l'on demande de faire ne fonctionnera pas et que cela créera une vulnérabilité.

Évidemment, de notre côté, nous avons des experts à l'intérieur du gouvernement qui nous ont aidés avec le projet de loi C-22 et qui connaissent ces enjeux. On peut continuer de faire appel à leurs services pour nous aider dans l'élaboration et pour travailler de concert avec les fournisseurs.

La sénatrice Youance : On imagine qu'il y aura un bon nombre d'informations dans l'application du projet de loi C-22. Est-ce que, au niveau des ministères, vous évaluez la possibilité d'utiliser l'intelligence artificielle pour analyser ces données? Encore une fois, quelles seraient les balises?

M. Bilodeau : Il est important de souligner que le gouvernement ne détiendra aucune de ces informations. L'information qui pourrait être retenue par des fournisseurs, dont les métadonnées, ne sera pas détenue par le gouvernement. Nous ne sommes pas intéressés à l'avoir. Il s'agit de l'information des gens. La seule situation où une entité gouvernementale pourrait accéder à ces informations requiert un mandat de perquisition émis par un tribunal et serait exécuté par un service de police. À ce moment-là, certaines balises protégeraient cette information.

La sénatrice Youance : Merci beaucoup.

[*Traduction*]

Le sénateur Dalphond : J'ai deux questions.

[*Français*]

La première est pour M. Bilodeau et la deuxième pour Mme Gibner.

Monsieur Bilodeau, vous avez peut-être entendu des témoins précédents qui ont demandé d'ajouter le principe de proportionnalité au sujet des ordonnances ministérielles. Est-ce que cela vous créerait un problème si l'on ajoutait cette notion en la rendant plus expresse qu'implicite?

M. Bilodeau : Si l'on regarde les critères actuels, c'est certainement implicite. Monsieur Noël l'a mentionné, c'est ce qu'il ferait avec l'information. Au moins, de manière implicite, on s'attend à ce que cette analyse soit faite. À savoir si l'on peut la mettre dans la législation et la position de mon ministre, ce sont des discussions que nous pourrons avoir avec lui. Au fur et à mesure que le processus continue, nous aurons l'occasion de revenir — je le souhaite — et nous pourrons en discuter à ce moment-là.

Le sénateur Dalphond : Merci.

[*English*]

Ms. Gibner, could an order for subscriber information be addressed to a daycare or health authority? The minister said information held by health providers or medical information is protected, and the same is true for informants and lawyers. My question is more about the scope of what is intended here. Would it be possible to use that provision to ask a nurse or kindergarten provider that communicates with parents through a web service to be a service provider as contemplated here?

Ms. Gibner: If it is all right with you, I'll pass that question to Ms. Lebel.

[*Translation*]

Ms Anne-Marie Lebel, Counsel, Criminal Law Policy Section, Department of Justice Canada: Thank you very much for the question.

Your question could pertain to Part 1 or Part 2 of the bill.

Senator Dalphond: Part 1.

Ms. Lebel: In the case of Part 1, a production order for the subscriber information could be made to any service provider, to anyone who provides services to the public. That could be a daycare in some cases, but the conditions for obtaining such orders are related to an investigation. The judge must be convinced that there are reasonable grounds to believe that an offence was committed and that asking for the information of the subscriber or client would help the investigation. The criteria are there. A daycare cannot just be asked any question for any reason. The provision sets out the conditions for obtaining the order.

It is also important to note that the new production order for subscriber information is actually more limited in scope than the other orders under the Criminal Code. The other production orders under the Criminal Code can be made and presented to any person who is in possession or control of information related to the investigation. The scope is already more limited than that of the other orders. Does that answer your question?

Senator Dalphond: Would the other orders be made with reasonable grounds to believe?

Ms. Lebel: Not necessarily. There are currently several examples of production orders in the Criminal Code that are obtained on the basis of reasonable grounds to suspect, for

[*Traduction*]

Madame Gibner, pourrait-on adresser une ordonnance pour l'obtention des renseignements sur l'abonné à une garderie ou à une autorité de la santé? Le ministre a dit que les renseignements détenus par les prestataires de soins de santé ou les renseignements médicaux sont protégés, et qu'il en va de même pour les informateurs et les avocats. Ma question porte davantage sur la portée de ce qui est prévu ici. Serait-il possible d'utiliser cette disposition pour demander à une infirmière ou à une éducatrice de maternelle qui communique avec les parents par l'intermédiaire d'un service Web d'agir à titre de fournisseur de services au sens où on l'entend ici?

Mme Gibner : Si vous le permettez, je vais transmettre cette question à Me Lebel.

[*Français*]

Me Anne-Marie Lebel, avocate, Section de la politique en matière de droit pénal, Ministère de la Justice Canada : Merci beaucoup de la question.

Votre question pourrait toucher à la partie 1 ou 2 du projet de loi.

Le sénateur Dalphond : La partie 1.

Me Lebel : Dans le cas de la partie 1, effectivement, une ordonnance de communication pour les renseignements de l'abonné pourrait être faite à n'importe quel fournisseur de services, une personne qui fournit des services au public. Cela pourrait être une garderie dans certains cas, mais les conditions pour obtenir ces ordonnances sont reliées à une enquête. Le juge doit être convaincu qu'il a des motifs raisonnables de croire qu'une infraction a été commise, et qu'en demandant l'information de l'abonné ou du client, que cela aidera l'enquête. Les critères sont là. On ne peut pas poser n'importe quelle question à un service de garde pour n'importe quel objectif. Les conditions d'obtention de l'ordonnance sont donc dans la disposition.

Il est important de noter également que la nouvelle ordonnance de communication pour les renseignements de l'abonné est, dans les faits, plus limitée en matière de portée que les autres ordonnances du Code criminel. Les autres ordonnances de communication du Code criminel peuvent être faites et présentées à n'importe quelle personne qui se trouve en possession de contrôle de renseignements qui sont pertinents à l'enquête. C'est déjà une portée plus restrictive que les autres ordonnances. Est-ce que cela répond à votre question?

Le sénateur Dalphond : Les autres ordonnances seraient avec des motifs raisonnables de croire?

Me Lebel : Pas nécessairement. Actuellement, dans le Code criminel, il y a plusieurs exemples d'ordonnances de communication qui sont obtenues sur la base de motifs

example, location data and data concerning the transmission of financial information.

Senator Dalphond: Thank you.

[*English*]

The Chair: That completes the first round of our third session this evening.

I'll take the chair's prerogative to ask this question at this time. It is general to all of you. In listening to the past three hours, I've noticed some of the lanes of expertise at the table are complementary and overlapping and some are unique, whether they are in the field, in policy or in criminal law. I would like to give you the opportunity to add to your testimony if you have not shared something that will make this story complete for us as senators, since we may not get to see you again in the next little while. Is there anything missing from your testimony, from your perspective, that you want to make sure you emphasize for us this evening that you might not have had a chance to? I invite you to consider doing that now.

Ramzi Nashef, Director General, Policy, Planning, and Accountability, Canadian Security Intelligence Service: We talked about some of the RCMP and law enforcement examples, but maybe I can give you an intelligence perspective. From CSIS's perspective, the emphasis is on Part 2. At the end of the day, we feel, if passed as written now, Part 2 will take us out of the space we are in.

To get back to Senator Cardozo's question about whether we have some lawful access in Canada, the short answer is yes. However, it's incredibly ad hoc. From an operational planning perspective, what we get, even when we have a Federal Court warrant, is incredibly heavy, unstable and unpredictable in different parts of this country and with different service providers regionally.

What we would get with Part 2 is a strong starting point for us to know what to expect operationally. That means less front-end planning of operations among intelligence professionals. It means less operational uncertainty. It means fewer inconsistent and unpredictable investigative outcomes. At the end of the day, the investigative outcome component, for us, is the difference between a successful and a dropped investigation regarding the most harmful threats in the national security space. Essentially, we're talking about foreign interference, espionage and terrorism, primarily.

raisonnables de soupçonner, par exemple, les données de localisation et les données de transmission des données financières également.

Le sénateur Dalphond : Merci.

[*Traduction*]

La présidente : Cela conclut la première série de notre troisième heure aujourd'hui.

Je vais faire usage de la prérogative du président pour poser cette question à présent. Elle s'adresse à vous tous de manière générale. En écoutant les trois dernières heures, j'ai remarqué que certains domaines d'expertise représentés à cette table sont complémentaires et se recoupent, tandis que d'autres sont uniques, qu'ils relèvent du terrain, des politiques ou du droit criminel. J'aimerais vous accorder l'occasion de compléter votre témoignage si vous n'avez pas encore abordé un élément qui permettrait de brosser un tableau complet de la situation pour nous, sénateurs, car il se peut que nous n'ayons pas l'occasion de vous revoir avant un certain temps. Y a-t-il, selon vous, un élément manquant dans votre témoignage que vous souhaitez absolument souligner ce soir et que vous n'avez peut-être pas eu l'occasion d'évoquer? Je vous invite à le faire maintenant.

Ramzi Nashef, directeur général, Politique, planification et responsabilité, Service canadien du renseignement de sécurité : Nous avons cité certains exemples concernant la GRC et les forces de l'ordre, mais je pourrais peut-être vous présenter un point de vue du renseignement. Du point de vue du SCRS, l'accent est mis sur la partie 2. En fin de compte, nous estimons que, si elle est adoptée telle qu'elle est rédigée actuellement, la partie 2 nous fera sortir de la situation dans laquelle nous nous trouvons.

Pour revenir à la question du sénateur Cardozo visant à savoir si nous disposons d'un accès légal au Canada, en bref, la réponse est oui. Cependant, cet accès est extrêmement ponctuel. Du point de vue de la planification opérationnelle, ce à quoi nous avons accès, même si nous sommes munis d'un mandat de la Cour fédérale, est extrêmement lourd, instable et imprévisible selon les régions du pays et les différents fournisseurs de services.

Ce que nous obtiendrions avec la partie 2, c'est un point de départ solide qui nous permettrait de savoir à quoi nous attendre sur le plan opérationnel. Cela signifie moins de planification initiale des opérations pour les professionnels du renseignement. Cela signifie moins d'incertitude opérationnelle. Cela signifie moins de résultats d'enquête incohérents et imprévisibles. En définitive, pour nous, la composante « résultat de l'enquête » représente toute la différence entre une enquête couronnée de succès et une enquête sur des menaces très graves dans le domaine de la sécurité nationale, qui est abandonnée. Essentiellement, nous parlons principalement d'ingérence étrangère, d'espionnage et de terrorisme.

Really, that's the starting point that all like-minded partners — well beyond the G7 and the Five Eyes and into medium and small European countries, for example — have had, in many cases, for more than a decade, which we've really struggled to cobble together in different ways to sort of get the job done. The amount of effort and the amount of uncertainty that's created operationally have been significant. Maybe I will leave it there.

En réalité, c'est le point de départ dont disposent depuis plus d'une décennie tous les partenaires aux vues similaires — bien au-delà du G7 et du Groupe des cinq, jusqu'aux pays européens de taille moyenne et petite, par exemple —, ce que nous avons eu beaucoup de mal à mettre en place de différentes façons pour, en quelque sorte, mener à bien notre mission. L'ampleur des efforts déployés et le degré d'incertitude qui en a résulté sur le plan opérationnel ont été considérables. Je m'arrêterai peut-être là.

The Chair: Thank you. You jumped in there, and I really appreciate it. My follow-up with that, with you, is this: In Canada, I would say that Canadians are expressing their discomfort, regarding business and otherwise, in section 2. I'm just going to talk about section 2. As a closing question for you, how do we calm, respectfully, folks who really feel that section 2 will paralyze their world?

La présidente : Merci. Vous avez pris la parole, et je vous en suis très reconnaissante. Ma question complémentaire à ce sujet, qui s'adresse à vous, est la suivante. Au Canada, je dirais que les Canadiens expriment leur malaise, tant sur le plan des affaires que sur d'autres plans, concernant l'article 2. Je vais me limiter à parler de l'article 2. Pour conclure, comment pouvons-nous rassurer, avec respect, les gens qui ont vraiment l'impression que l'article 2 va paralyser leur vie?

Mr. Nashef: It is a great question. I think we have some really good case studies to look at in terms of the like-mindeds, as I said. When we're sort of last in line, we have a lot of examples to look at regarding what was mythology and what actually came to pass.

M. Nashef : C'est une excellente question. Je pense que nous disposons de très bonnes études de cas à examiner en ce qui concerne les entités aux vues similaires, comme je l'ai dit. Même si nous sommes en quelque sorte les derniers de la file, nous avons de nombreux exemples à examiner concernant ce qui relevait du mythe et ce qui s'est réellement produit.

In combination with the House Committee on Public Safety and National Security study that went in-depth and where officials on this side appeared, through clause by clause, for upwards of 20 or 25 hours — and they answered a huge depth of questions — I think, ultimately, where we have a bit of a challenge is there are strong views on both sides of this bill, as you all know even better than we do. Ultimately, the proof will be in the pudding in a lot of cases.

Si l'on ajoute à cela l'étude approfondie menée par le comité de la Chambre des communes sur la sécurité publique et nationale — au cours de laquelle de hauts fonctionnaires de notre côté ont comparu pendant plus de 20 ou 25 heures d'examen article par article, et ont répondu à une multitude de questions très détaillées —, je pense qu'en fin de compte, notre principal défi réside dans le fait qu'il existe des opinions très tranchées des deux côtés sur ce projet de loi, comme vous le savez tous encore mieux que nous. En fin de compte, c'est à l'usage que l'on jugera de la valeur de ce projet de loi dans bien des cas.

Some of the maximalist interpretations of this bill in terms of saying that it will be the end of x, y and z, or that it will create a surveillance state in ways that go well beyond — I think we've seen a lot of examples where that came to pass, and it has been a bit of a fizzle, to be frank. Looking at those examples, what it should counsel for us is, certainly, deep study and appreciation for the scale of what we're talking about and for the privacy rights at stake, but also to look at what might have been hyperbole that really didn't get realized in a lot of key partner countries — not that that's the end of the conversation, though.

Certaines opinions maximalistes avancent que ce projet de loi signifie la fin de x, y et z, ou qu'il créerait un État de surveillance à un degré bien supérieur à ce qui est prévu. Nous avons vu de nombreux exemples où cela s'est produit, et qui, franchement, se sont avérés être un peu un coup d'épée dans l'eau. Analyser ces exemples devrait nous inciter à examiner ce projet de loi en profondeur et à bien saisir l'ampleur de ce dont nous parlons, ainsi que les droits à la vie privée en jeu. Il devrait aussi nous encourager à reconnaître ce qui aurait pu être de l'exagération et qui ne s'est finalement pas concrétisé dans de nombreux pays partenaires clés, ce qui ne signifie pas, en fin de compte, que le débat est clos.

The Chair: Thank you so much. I'm glad I asked. Is there anyone else? Yes, sir.

La présidente : Merci beaucoup. Je suis heureuse d'avoir posé cette question. Y a-t-il quelqu'un d'autre? Oui, monsieur.

Mr. Burchill: Thank you, chair. I just want to underscore some things in our parliamentary appearances here that don't always get focused on. When we give operational examples, a lot of times, we provide examples that are dealing with one issue.

M. Burchill : Merci, madame la présidente. Je voudrais simplement souligner certains aspects de nos comparutions parlementaires ici qui ne retiennent pas toujours l'attention. Lorsque nous donnons des exemples opérationnels, nous citons

Something I wanted to highlight that supports the timeliness and the consistency of access is the complexity of the file.

So, to my colleague's example earlier, it is not just one IP address or number you're generally looking for. When we're dealing with major transnational organized crime files, extortion files and national security files, there are multiple targets in these files. So you multiply all the things we're talking about and the timeliness that we need access by many. I don't think the volume and complexity of investigations always get captured in committee with folks.

Then there is the volume of files. I'll use the example of our National Child Exploitation Centre. As of today, because I asked them what the intake unit is at, they are 24,700 files behind. A lot of that is just trying to get through that volume and get timely investigative evidentiary packages out to police in the jurisdiction. I don't think those things always get captured by the operational examples we use, and I wanted to highlight those in relation to the two parts of the bill.

The Chair: That is so important. Thank you. That's why I asked. That's great. I think we're good across the rest of the table, except for Mr. Bilodeau.

Mr. Bilodeau: I may pick up on something he said. You asked about Canadians. I think the minister highlighted where our efforts are going to be concentrated regarding core providers, and that is on the three categories we mentioned earlier. The rules around that are about facilitating access. They are about making sure that when police or CSIS go in, the providers can provide the information. With the metadata, there is a lot of information that's stored already by a lot of companies. They all take cybersecurity very seriously already, regardless of this legislation.

The safeguards that have been put in place are really meant to balance privacy and security. It is important to highlight that, because it is not about creating direct access or things like that. It is about creating the conditions so that when these folks have a need for the information, they can really quickly dial into that and get the information consistently. That's something where we need to take a step back sometimes and look practically at what this is going to mean. To your point, Senator Youance, it is about making sure that we have the right framework so we can pivot in the future as well.

The Chair: Thank you very much for that.

souvent des cas qui ne portent que sur un seul enjeu. Je voudrais mettre l'accent sur un élément qui confirme la pertinence et la cohérence de l'accès : la complexité du dossier.

Ainsi, pour reprendre l'exemple donné tout à l'heure par mon collègue, ce n'est généralement pas une seule adresse IP ou un seul numéro que l'on recherche. Lorsque nous traitons de dossiers importants liés au crime organisé transnational, à l'extorsion ou à la sécurité nationale, ces dossiers comportent de multiples cibles. Il faut donc multiplier par plusieurs tous les éléments dont nous parlons, ainsi que l'urgence avec laquelle nous avons besoin d'y avoir accès. Je crois que les gens ne saisissent pas toujours l'ampleur et la complexité des enquêtes.

Il y a ensuite le nombre de dossiers. Je vais prendre l'exemple de notre Centre national de coordination contre l'exploitation des enfants. À ce jour, d'après ce qu'ils m'ont indiqué, ils ont 24 700 dossiers qui accusent un retard. Une grande partie de ce travail consiste simplement à traiter ce volume et à transmettre en temps opportun les dossiers de preuve aux forces de l'ordre de l'administration concernée. Je ne pense pas que ces aspects soient toujours pris en compte dans les exemples opérationnels que nous utilisons, et je tenais à les souligner en lien avec les deux volets du projet de loi.

La présidente : C'est extrêmement important. Merci. C'est pour cela que j'ai posé la question. C'est très bien. Je pense que tout le monde autour de la table est d'accord, à l'exception de M. Bilodeau.

M. Bilodeau : Je voudrais revenir sur un de ses points. Vous avez posé une question au sujet des Canadiens. Je crois que le ministre a précisé sur quoi nos efforts allaient se concentrer en ce qui concerne les principaux fournisseurs, à savoir les trois catégories que nous avons mentionnées plus tôt. Les règles à cet égard visent à faciliter l'accès. Elles visent à garantir que, lorsque la police ou le SCRS interviennent, les fournisseurs puissent fournir l'information. En ce qui concerne les métadonnées, de nombreuses entreprises stockent déjà une grande quantité d'informations. Elles prennent toutes déjà la cybersécurité très au sérieux, indépendamment du projet de loi.

Les mesures de protection mises en place visent réellement à trouver un équilibre entre la vie privée et la sécurité. C'est important de le souligner, car il ne s'agit pas de créer un accès direct ou quelque chose du genre. Il s'agit de créer les conditions pour que, lorsque ces intervenants ont besoin de ces renseignements, ils puissent y accéder très rapidement et les obtenir systématiquement. Sur ce point, nous devons parfois prendre du recul et examiner concrètement ce que cela va signifier. Pour répondre à votre observation, sénatrice Youance, il s'agit de s'assurer que nous disposons du cadre approprié afin de pouvoir également nous adapter à l'avenir.

La présidente : Merci beaucoup de ces précisions.

We have some more questions, which is great. We have four senators, Senators Cardozo, Ross, Martel and Dalphond, who have joined us for the final round. I will ask Senator Cardozo and Senator Ross to give us your questions. Then we can get those answers. If you could, please ask those first, back to back.

Senator Cardozo: I want to pursue the last question that Madam Chair asked a little more. When requiring lawful access to information, what is the role of the RCMP versus CSIS? Are you often on the same files?

The other question I have for Mr. Bilodeau is this: You talked about this being technology neutral in terms of what you're looking at. Are you thinking about AI down the road — and it may not be very far down the road — where it may be a bad actor on its own and not driven by anyone?

Senator Ross: I understand that some Taiwanese cyber experts and some emerging technology researchers have been invited as witnesses as part of this study. Taiwan faces 2.6 sophisticated cyberattacks every day and deals with extreme risks related to encryption issues. I'm wondering if the government has looked at their approach to governance, resilience and cybersecurity to incorporate into this framework. If not, what other international models have we looked at for guidance?

Mr. Bilodeau: Maybe I can start with your question first. The answer on lawful access and, specifically, the Taiwanese, is no. However, just generally, on cyber resilience, Parliament, as you know, passed Bill C-8 this summer, and it received Royal Assent. This is the legislation about protecting cyber systems and critical infrastructure. I think that's a very important piece of legislation that will increase the protection of critical infrastructure in this country from cybersecurity threats. We know, especially in the age of AI, that the threat is increasing. The Canadian Centre for Cyber Security, or CCCS, has spoken about it, so it is a constant battle. There are billions of attacks on systems happening all the time. There is a separate piece of legislation, and that's what we are focused on implementing now.

It is not just us. It is the private sector, and it is provincial, territorial and municipal governments. Everybody takes this seriously. We try to partner and help as much as we can on that. Again, this legislation is going to live alongside that. The systemic vulnerability provision is designed to make sure we're not weakening the system while we implement this legislation.

Nous avons encore quelques questions, ce qui est excellent. Quatre sénateurs se sont joints à nous pour cette dernière série de questions : les sénateurs Cardozo, Martel et Dalphond et la sénatrice Ross. Je vais demander à la sénatrice Ross et au sénateur Cardozo de nous présenter leurs questions. Nous pourrons ensuite entendre les réponses. Si possible, posez-les l'une après l'autre.

Le sénateur Cardozo : J'aimerais approfondir un peu plus la dernière question posée par madame la présidente. Lorsqu'il s'agit d'exiger un accès légal à l'information, quel est le rôle de la GRC par rapport à celui du SCRS? Travaillez-vous souvent sur les mêmes dossiers?

L'autre question que j'ai à l'intention de M. Bilodeau est la suivante : vous avez mentionné que votre approche était technologiquement neutre en ce qui concerne ce que vous examinez. Envisagez-vous, dans un avenir peut-être plus proche que vous ne le pensez, que l'intelligence artificielle puisse agir de manière malveillante de son propre chef, sans être pilotée par qui que ce soit?

La sénatrice Ross : Je crois comprendre que certains cyberexperts taïwanais et certains analystes en technologies émergentes ont été invités à témoigner dans le cadre de cette étude. Taïwan fait face à 2,6 cyberattaques complexes chaque jour et doit composer avec des risques extrêmes liés aux problèmes de chiffrement. Je me demande si le gouvernement a examiné leur approche en matière de gouvernance, de résilience et de cybersécurité afin de l'intégrer à ce cadre. Si ce n'est pas le cas, quels autres modèles internationaux avons-nous étudiés pour nous guider?

M. Bilodeau : Je peux peut-être répondre en premier à votre question. Concernant l'accès légal, et plus précisément le cas de Taïwan, la réponse est non. Toutefois, en général, concernant la cyberrésilience, comme vous le savez, le Parlement a adopté cet été le projet de loi C-8 qui a reçu la sanction royale. Il vise à protéger les cybersystèmes et les infrastructures essentielles. Selon moi, c'est une mesure législative très importante qui renforcera la protection des infrastructures essentielles du pays contre les menaces de cybersécurité. Nous savons que la menace s'intensifie, surtout à l'ère de l'IA. Le Centre canadien pour la cybersécurité, ou CCC, en a parlé; il s'agit donc d'une lutte constante. Les systèmes sont sans cesse la cible de milliards d'attaques. Il existe une loi distincte et nous nous penchons sur sa mise en œuvre.

Nous ne sommes pas les seuls concernés. Le secteur privé ainsi que les gouvernements provinciaux, territoriaux et municipaux sont également concernés. Tout le monde prend cette question au sérieux. Nous essayons de nouer des partenariats et d'apporter toute l'aide possible à cet égard. Encore une fois, ce projet de loi s'inscrit dans ce cadre. La disposition relative aux vulnérabilités systémiques vise à garantir

On AI, yes, it is something that we are focused on every day. It is hard not to when it is constantly in the media and we see example after example. Right now, in terms of whether AI would be subject to a ministerial order or a core provider, I think time will tell how services that use AI evolve. However, right now, the focus is trying to establish that baseline and raise everybody's "floor" — as I think Ramzi said at some point at the House Committee on Public Safety and National Security — to a level where when these folks go to them and need information, they can respond to them. I will go to the RCMP for the first question.

Mr. Burchill: My colleague at CSIS can jump in to supplement. We have different mandates, but our mandates cross when we have a national security investigation. However, we're doing them for very different reasons. In a criminal investigation, of course, everything we do is done through the courts, is disclosable and goes through the court process. CSIS does it in a separate sort of process that's in secret because of the nature of what they do. So we're using the same legislation but for different Band-Aids, if that helps.

By the very nature of what we do, our Band-Aids cross in a national security investigation, but for different reasons. And there are ways to hand off to one another when it is not a law enforcement mandate part of the investigation or vice versa; if it is not a security intelligence mandate, they hand it off. There are mechanisms for that. However, as far as this legislation goes, we would use them in parallel and for different mandates.

[*Translation*]

Senator Martel: I would like to come back to the service providers. Bill C-22 provides that the minister can grant financial compensation to service providers to meet certain technical obligations. What criteria will be used to determine whether a provider receives such compensation?

Senator Dalphond: Part 2 comes into force by order of the Governor-in-Council and Part 1 comes into force six months after royal assent. Since this is a major undertaking, the framework is there, but everything else will be done later through government regulations. What deadline do you have in mind? You will have to consult, publish, review and republish. I read that some critics are saying that Part 2 will not take effect for two or three years. Is that possible?

que nous n'affaiblissons pas le système pendant la mise en œuvre de cette loi.

En ce qui concerne l'IA, oui, c'est un sujet sur lequel nous nous penchons quotidiennement. Difficile de faire autrement alors que les médias en parlent sans cesse et que les exemples se multiplient. À l'heure actuelle, à savoir si l'IA relèverait d'un arrêté ministériel ou d'un fournisseur principal, je pense que le temps nous dira comment évolueront les services qui utilisent l'IA. Cependant, pour l'instant, l'objectif est d'établir ce niveau de base et de relever le « seuil minimal » de tout le monde — comme Ramzi Nashef l'a dit un jour, je crois, au Comité permanent de la sécurité publique et de la sécurité nationale de la Chambre des communes — à un niveau tel que, lorsque ces personnes s'adressent à eux et demandent de l'information, ils puissent leur répondre. Je vais céder la parole à la GRC pour la première question.

M. Burchill : Ma collègue du SCRS peut intervenir pour compléter mes propos. Nos mandats sont différents, mais ils se recoupent lorsque nous menons une enquête de sécurité nationale. Toutefois, nous menons ces enquêtes pour des raisons très différentes. Dans une enquête criminelle, bien sûr, tout ce que nous faisons passe par les tribunaux, est susceptible d'être divulgué et suit la procédure judiciaire. Le SCRS, quant à lui, procède selon un processus distinct qui se déroule en secret en raison de la nature de ses activités. Nous utilisons donc la même loi, mais pour des « remèdes » différents, si cela peut aider.

En raison de la nature même de nos activités, nos mandats se recoupent dans le cadre d'une enquête de sécurité nationale, mais pour des raisons différentes. Et il existe des moyens de se passer le relais lorsque l'enquête ne relève pas d'un mandat d'application de la loi, ou inversement; s'il ne s'agit pas d'un mandat de renseignement de sécurité, ils nous transfèrent le dossier. Des mécanismes sont prévus à cet effet. Toutefois, en ce qui concerne ce projet de loi, nous exercerions nos pouvoirs en parallèle et pour des mandats différents.

[*Français*]

Le sénateur Martel : J'aimerais revenir aux fournisseurs. Dans le projet de loi C-22, on prévoit que le ministre pourrait accorder une compensation financière aux fournisseurs pour respecter certaines obligations techniques. Quels critères permettront de déterminer si un fournisseur pourrait bénéficier de cette compensation?

Le sénateur Dalphond : La partie 2 entre en vigueur par décret du gouvernement et la partie 1 entre en vigueur six mois après la réception de la sanction royale. Puisque c'est un grand paramètre, l'ossature est là, mais tout le reste arrivera après par règlement du gouvernement. Quel échéancier avez-vous en tête? Il faut consulter, publier, prendre connaissance, republier. J'ai lu que certains critiques disent que la partie 2 ne sera pas en vigueur avant deux ou trois ans. Est-ce possible?

Mr. Bilodeau: Thank you.

I will start with Senator Martel's question about service providers. One thing we need to consider when implementing the bill is how compensation will be handled, for both core providers and for orders. We will have to look at what is appropriate. It is difficult to say what the criteria will be. In cases where the capability does not currently exist, it could be more expensive. We will have to assess the situation as we go and as we work with the service providers to understand their needs.

With regard to the coming into force, our timeline is much shorter than two years. We understand that law enforcement has been waiting for these tools for nearly 35 or 40 years. We are already thinking about developing and implementing these regulations in well under two years.

Senator Dalphond: Will it be before the parliamentary review in three years?

Mr. Bilodeau: Absolutely.

Senator Dalphond: Thank you.

[*English*]

Senator Pate: Many cybersecurity experts, as well as stakeholders such as telecommunications and internet service providers, have argued that any introduction of mandatory data access capabilities will create systemic vulnerabilities that will inevitably be targeted and breached by bad actors.

I'm curious as to the provision that's put in place by the act. It establishes that any service provider who does not comply with a regulation or order can be subject to significant fines for every day of non-compliance. So, I'm curious how a service provider could push back against a measure they determine would create systemic vulnerability while under such a threat.

Also, the scope of "electronic service and electronic service provider" seems extraordinarily wide, and I'm curious as to why it needs to be that wide. How would there be some protection in terms of the scope for booking services, retail platforms, banks and so on? I'm not sure who could best answer.

Mr. Bilodeau: On your first question, we want to work with service providers to understand, and they know their systems best. When we put forward regulations, we'll consult and work with them to understand their systems. It is the same thing with ministerial orders; we have to work with the electronic service providers to understand what those concerns are. The goal is not to issue administrative monetary penalties against them for

M. Bilodeau : Merci.

Je commencerai avec la question du sénateur Martel concernant les fournisseurs. Un des éléments de la mise en œuvre du projet de loi sera de regarder comment on considère la compensation, que ce soit pour les fournisseurs principaux, mais aussi pour les ordonnances. Il s'agira de voir ce qui est approprié. Il est difficile de dire quel sera le critère. S'il s'agit d'une capacité qui n'existe pas, cela peut être plus dispendieux. Nous devrons voir au fur et à mesure et en travaillant avec les fournisseurs pour comprendre leurs besoins.

Concernant l'entrée en vigueur, notre échéancier est plus beaucoup plus court que deux ans. On comprend que les forces de l'ordre ont besoin de ces outils depuis près de 35 ou 40 ans. On est déjà à penser à la mise en œuvre et de développer des règlements bien en deçà de deux ans.

Le sénateur Dalphond : Est-ce que ce sera avant que l'on procède à la revue parlementaire dans trois ans?

M. Bilodeau : Absolument.

Le sénateur Dalphond : Merci.

[*Traduction*]

La sénatrice Pate : De nombreux experts en cybersécurité et d'autres intervenants, notamment les fournisseurs de services de télécommunications et d'Internet, ont fait valoir que toute mesure rendant obligatoire l'accès aux données créerait des vulnérabilités systémiques qui seraient inévitablement ciblées et exploitées par des acteurs malveillants.

Je suis curieuse de connaître la disposition prévue par la loi. Elle stipule que tout fournisseur de services qui ne se conforme pas à un règlement ou à une ordonnance peut se voir infliger des amendes importantes pour chaque jour de non-conformité. Je me demande donc comment un fournisseur de services pourrait s'opposer à une mesure qu'il estime susceptible de créer une vulnérabilité systémique s'il s'expose à une telle menace.

De plus, la portée des termes « services électroniques » et « fournisseur de services électroniques » semble extraordinairement large, et je me demande pourquoi elle doit l'être à ce point. Comment pourrait-on assurer une certaine protection en ce qui concerne la portée de ces dispositions pour les services de réservation, les plateformes de vente au détail, les banques, etc.? Je ne sais pas exactement qui serait le mieux placé pour répondre à cette question.

M. Bilodeau : Concernant votre première question, nous souhaitons collaborer avec les fournisseurs de services pour mieux comprendre leurs systèmes, car ce sont eux qui les connaissent le mieux. Quand nous proposerons des règlements, nous les consulterons et travaillerons avec eux pour comprendre leurs systèmes. Il en va de même pour les arrêtés ministériels : nous devons collaborer avec les fournisseurs de services

non-compliance. Our goal is to get to a point where they can put in place capabilities that allow law enforcement and CSIS to get access when they have judicially authorized warrants to do so. Compliance regimes are common for these kinds of frameworks. It is kind of the backbone. It is the thing you want there backstopping things, to make sure there's compliance, but that you don't want to use. You want to make sure you're doing it collaboratively.

At the end of the day, if they can meet the needs of the legislation and law enforcement in a way that's secure, respects the legislation on systemic vulnerability and gives law enforcement access when they need it, that's the goal we're looking to achieve.

I'm sorry, senator. What was the second part of the question regarding?

Senator Pate: The scope of the definition of "electronic service and electronic service provider" seems extraordinarily wide.

Mr. Bilodeau: I will ask Ms. Hiegel to answer.

Shannon Hiegel, Director General, National and Cyber Security Branch, Public Safety Canada: Thanks very much for the question. It is one that we get quite frequently when people are trying to understand why we're as broad as we are. It is probably where we're leaning the most forward when we look at the comparisons across all the countries we've taken a look at. However, the fact of the matter is that our definition would at least include things like gaming platforms, where communication isn't the primary purpose of that service but there is a predominant chat room and chat function. I suppose I shouldn't name names, but there are certain gaming platforms where we know there is child grooming and there are human trafficking discussions. So if we don't allow for the flexibility — I think there have been other senators asking questions about how we ensure that we are technology-focused and forward-leaning in this space. That's where we have made a choice to at least present a definition that is quite broad.

Senator Pate: I know it is going to be a three-year review. In your experience, in the areas where legislation has been passed in the past — just pulling a number out of the air — 10 years, how often have those legislative reviews happened?

électroniques pour cerner leurs préoccupations. L'objectif n'est pas de leur imposer des sanctions administratives pécuniaires pour non-conformité. Notre objectif est d'en arriver à un point où ils pourront mettre en place des capacités permettant aux forces de l'ordre et au SCRS d'accéder aux données lorsqu'ils disposent de mandats autorisés par un tribunal. Les régimes de conformité sont courants dans ce genre de cadres. C'est en quelque sorte la colonne vertébrale. C'est ce que l'on souhaite avoir en arrière-plan pour garantir la conformité, mais que l'on ne souhaite pas utiliser. On veut s'assurer que tout se fait dans un esprit de collaboration.

En fin de compte, s'ils peuvent répondre aux exigences législatives et aux besoins des forces de l'ordre d'une manière sécuritaire, qui respecte la loi sur les vulnérabilités systémiques et qui accorde aux forces de l'ordre l'accès dont elles ont besoin, c'est l'objectif que nous cherchons à atteindre.

Je suis désolé, sénatrice Pate. Sur quoi portait la deuxième partie de la question?

La sénatrice Pate : La portée de la définition des « services électroniques » et des « fournisseurs de services électroniques » semble extraordinairement large.

M. Bilodeau : Je vais demander à Mme Hiegel de répondre.

Shannon Hiegel, directrice générale, Secteur de la sécurité nationale et de la cybersécurité, Sécurité publique Canada : Merci beaucoup pour cette question. Les gens nous la posent assez fréquemment lorsqu'ils tentent de comprendre pourquoi notre définition est aussi large. C'est probablement là que nous allons le plus loin lorsque nous comparons les différentes dispositions législatives de tous les pays que nous avons examinées. Cependant, le fait est que notre définition inclurait au moins des éléments comme les plateformes de jeux, où la communication n'est pas l'objectif principal du service, mais où l'on trouve une salle et une fonction de clavardage prédominantes. Je suppose que je devrais m'abstenir de citer des noms, mais nous savons que certaines plateformes de jeux donnent lieu à du leurre d'enfants et à des discussions sur la traite de personnes. Donc, si nous ne prévoyons pas cette souplesse — je crois que d'autres sénateurs ont posé des questions sur la façon dont nous nous assurons d'adopter une approche axée sur la technologie et tournée vers l'avenir dans ce domaine —, c'est là que nous avons choisi de présenter au moins une définition assez large.

La sénatrice Pate : Je sais qu'il y aura un examen triennal. D'après votre expérience, dans les domaines où des projets de loi ont été adoptés par le passé — prenons un chiffre au hasard — sur une période de 10 ans, à quelle fréquence ces examens législatifs ont-ils eu lieu?

Mr. Bilodeau: I know they happen. I wouldn't have a number. I know that with the Bank Act, for example, they happen every five years, but I wouldn't be able to give you a number.

Ms. Hiegel: For the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, or PCMLTFA, it is every five years, and Finance is diligent in doing it every five years.

Senator Pate: How about criminal law changes?

Ms. Hiegel: I would pass it over to my Justice colleagues for that question.

Ms. Gibner: We'd have to get back to you, Senator Pate. There is no specific review mechanism in the Criminal Code.

Senator Pate: No, but there are many pieces of legislation that have been passed over the past 10 years that required a 3-year or 5-year review that have not occurred. I'd be very interested in a catalogue of those. Thank you.

The Chair: Thank you to our panel. You do incredible work, and we really appreciate your time, frankly, in building on a three-hour opportunity for us this evening. I know some of you performed twice, so well done on that. We really appreciate it.

This brings us to the end of our time with witnesses. We are going to carry on. We want to thank you for taking the time with us today.

We are going to proceed with our clause-by-clause consideration of Bill S-223, An Act to amend the Royal Canadian Mounted Police Act.

I would also like to acknowledge and welcome Senator McCallum, who is joining us today. Thank you very much for that.

Before I begin, there are quite a few words, for sure. I would like to remind senators of a number of points as we proceed to clause-by-clause consideration.

If, at any point, a senator is not clear where we are in the process, please ask for clarification. I would like to ensure that, at all times, we have the same understanding of where we are. In terms of the mechanics of the process, when more than one amendment is proposed to be moved in a clause, amendments should be proposed in the order of the lines of the clause. If a senator is opposed to an entire clause, the proper process is not to move a motion to delete the entire clause, but rather to vote against the clause as standing as part of the bill.

M. Bilodeau : Je sais qu'ils ont lieu. Je ne pourrais pas vous donner de chiffre. Je sais que, dans le cas de la Loi sur les banques, par exemple, ils ont lieu tous les cinq ans, mais je ne serais pas en mesure de vous donner un chiffre.

Mme Hiegel : Pour la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, la LRPCFAT, c'est tous les cinq ans, et le ministère des Finances s'acquitte de cette tâche avec diligence tous les cinq ans.

La sénatrice Pate : Qu'en est-il des modifications au droit pénal?

Mme Hiegel : Je laisserais le soin à mes collègues du ministère de la Justice de répondre à cette question.

Mme Gibner : Nous devrons nous renseigner pour vous répondre, sénatrice Pate. Le Code criminel ne prévoit aucun mécanisme d'examen précis.

La sénatrice Pate : Non, mais de nombreux projets de loi adoptés au cours des 10 dernières années prévoyaient un examen tous les trois ou cinq ans, qui n'a pas eu lieu. J'aimerais beaucoup en avoir la liste. Merci.

La présidente : Merci à nos témoins. Vous faites un travail incroyable, et nous vous sommes sincèrement reconnaissants de prendre de votre temps pour enrichir cette séance de trois heures ce soir. Je sais que certains d'entre vous sont intervenus à deux reprises, alors bravo pour cela. Nous vous en sommes très reconnaissants.

Cela marque la fin de notre séance avec les témoins. Nous allons poursuivre nos travaux. Nous tenons à vous remercier d'avoir pris le temps de vous joindre à nous.

Nous allons maintenant procéder à l'étude article par article du projet de loi S-223, Loi modifiant la Loi sur la Gendarmerie royale du Canada.

J'aimerais également saluer et souhaiter la bienvenue à la sénatrice McCallum, qui se joint à nous aujourd'hui. Merci beaucoup d'être venue.

Avant de commencer, j'ai certainement des choses à vous dire. J'aimerais rappeler aux sénateurs un certain nombre de points alors que nous entamons l'étude article par article.

Si, à un moment donné, un sénateur ne sait pas où nous en sommes rendus dans le processus, veuillez demander des précisions. Je veux m'assurer que, en tout temps, nous comprenons tous où nous nous situons dans le processus. Pour ce qui est de la mécanique du processus, lorsque plus d'un amendement est proposé pour un article, les amendements devraient être présentés selon l'ordre des lignes de l'article. Si un sénateur s'oppose à un article complet, j'aimerais vous rappeler que, au comité, le processus approprié consiste à ne pas proposer

Some amendments that are moved may have consequential effects on the other parts of the bill. It is, therefore, useful to this process if a senator moving an amendment identifies to the committee other clauses in this bill where their amendment may have an impact. Otherwise, it would be very difficult for members of the committee to remain consistent in their decision making.

Because no notice is required to move amendments, there can, of course, have been no preliminary analysis of the amendments to establish which ones may be of consequence to others and which might be a little contradictory.

If committee members ever have any questions about the process or the proprietary of anything occurring, they can certainly raise a point of order. As chair, I will listen to arguments, decide when there has been sufficient discussion of a matter or order and make a ruling.

The committee is the ultimate master of its business within the bounds established by the Senate, and a ruling can be appealed to the full committee by asking whether the ruling shall be sustained.

I wish to remind honourable senators that if there's ever any uncertainty as to the result of a voice vote or a show of hands, the most effective route is to request a roll call vote, which, obviously, provides unambiguous results.

Finally, senators are aware that any tied vote negates the motion in question.

Is it agreed that the committee proceed to clause-by-clause consideration of Bill S-223, An Act to amend the Royal Canadian Mounted Police Act?

Hon. Senators: Agreed.

The Chair: Shall the title stand postponed?

Hon. Senators: Agreed.

The Chair: Shall clause 1 carry?

Hon. Senators: Agreed.

The Chair: Shall clause 2 carry?

Hon. Senators: Agreed.

The Chair: Shall the title carry?

Hon. Senators: Agreed.

de motion pour supprimer l'article au complet, mais plutôt de voter contre l'article, qui fait partie du projet de loi.

Certains amendements proposés peuvent avoir des effets corrélatifs sur d'autres parties du projet de loi. Si un sénateur souhaite proposer un amendement, il serait utile pour le processus qu'il mentionne au comité d'autres articles du projet de loi sur lesquels cet amendement pourrait avoir une incidence. Autrement, il sera difficile pour les membres du comité de rester cohérents dans leurs décisions.

Comme aucun préavis n'est nécessaire pour proposer des amendements, il se peut, bien sûr, qu'aucune analyse préliminaire des amendements n'ait été faite pour établir lesquels pourraient porter à conséquence pour d'autres et se révéler contradictoires.

Si des membres du comité ont des questions au sujet du processus, de la pertinence de ce qui se passe ici, ils peuvent assurément invoquer le Règlement. En tant que présidente, je vais écouter l'argument, déterminer s'il y a eu une discussion suffisante au sujet d'une affaire ou de la procédure et prendre une décision.

Le comité est le maître ultime de ses travaux dans les limites établies par le Sénat, et on peut porter en appel une décision devant le comité plénier en demandant si elle devrait être maintenue.

Je tiens à rappeler à tous les sénateurs que, en cas de doute sur les résultats d'un vote par oui ou par non ou d'un vote à main levée, le moyen le plus efficace est de demander un vote par appel nominal, qui produit un résultat sans ambiguïté.

Enfin, les sénateurs savent qu'une égalité des voix entraîne le rejet de la motion en question.

Est-il convenu de procéder à l'étude article par article du projet de loi S-223, Loi modifiant la Loi sur la Gendarmerie royale du Canada?

Des voix : D'accord.

La présidente : Êtes-vous d'accord de suspendre l'adoption du titre?

Des voix : D'accord.

La présidente : L'article 1 est-il adopté?

Des voix : D'accord.

La présidente : L'article 2 est-il adopté?

Des voix : D'accord.

La présidente : Le titre est-il adopté?

Des voix : D'accord.

The Chair: Thank you.

Shall the bill carry?

Hon. Senators: Agreed.

The Chair: Thank you.

Does the committee wish to consider appending observations to the report?

Senator Hay: Yes.

The Chair: Does the committee choose to stay in public for this part of the conversation? We will carry on in public. Thank you.

I have a name for one observation. Are there any other observations in the room?

Thank you.

I would welcome Senator Hay to speak to the observation.

Senator Hay: Before I begin, I want to thank Senator McCallum, the bill's sponsor, for her leadership on this legislation and the First Nations leaders who co-developed it with you. Thank you so much for that.

These observations that I'm putting forward are intended to strengthen the bill and ensure that its provisions are as effective as possible. I support Bill S-223.

Colleagues, I'm proposing that the committee append three observations to its report. They would follow a standard opening paragraph:

> Your committee held one meeting on 5 October 2026 and heard from 10 witnesses on the subject matter of Bill S-223, An Act to amend the Royal Canadian Mounted Police Act. The committee also received one written brief.

No witness opposed the objective of this bill, but we heard again and again that confirming the RCMP's duty is only the first step. These observations speak to what must come next.

I'll start with the most practical question we have heard in plain terms: Who pays for this? The committee:

> . . . notes that Bill S-223 would confirm the Royal Canadian Mounted Police's (RCMP's) duty to enforce First Nation laws but is silent on any potential additional funding requirements to meet the objectives of Bill S-223. The committee heard that the RCMP already faces significant resource pressures and that, without adequate policing and enforcement resources, First Nation communities could

La présidente : Merci.

Le projet de loi est-il adopté?

Des voix : D'accord.

La présidente : Merci.

Est-ce que le comité veut annexer des observations au rapport?

La sénatrice Hay : Oui.

La présidente : Le comité choisit-il de poursuivre en séance publique pour cette partie de la discussion? Nous allons poursuivre en séance publique. Merci.

J'ai un nom pour une observation. Y a-t-il d'autres observations dans la salle?

Merci.

J'invite la sénatrice Hay à prendre la parole au sujet de cette observation.

La sénatrice Hay : Avant de commencer, je tiens à remercier la sénatrice McCallum, la marraine du projet de loi, pour son leadership sur ce projet de loi, ainsi que les dirigeants des Premières Nations qui l'ont élaboré conjointement avec vous. Merci beaucoup.

Les observations que je présente visent à renforcer le projet de loi et à garantir que ses dispositions soient aussi efficaces que possible. J'appuie le projet de loi S-223.

Chers collègues, je propose que le comité ajoute trois observations à son rapport. Elles suivraient un paragraphe d'introduction standard :

> Votre comité a tenu une réunion le 5 octobre 2026 et entendu 10 témoins sur la teneur du projet de loi S-223, Loi modifiant la Loi sur la Gendarmerie royale du Canada. Il a également reçu un mémoire écrit.

Aucun témoin ne s'est opposé à l'objectif de ce projet de loi, mais nous avons entendu à maintes reprises que la confirmation de l'obligation de la GRC n'est qu'une première étape. Ces observations portent sur ce qui doit suivre.

Je commencerai par la question la plus concrète qui nous a été posée en termes clairs : qui paie pour cela? Le comité constate :

> [...] constate que le projet de loi S-223 confirmerait l'obligation de la Gendarmerie royale du Canada (GRC) de faire respecter les lois des Premières Nations, mais qu'il ne fait aucunement mention des besoins éventuels en matière de financement supplémentaire pour atteindre les objectifs dudit projet de loi. Le comité a entendu que la GRC doit déjà faire face à des contraintes importantes en matière de

> continue to experience challenges in the enforcement of their laws. The committee therefore strongly encourages the Government of Canada to assess the potential additional resources required so that the RCMP can enforce First Nation laws effectively.

Furthermore, Chief Louie of the First Nations Lands Advisory Board told us plainly that the RCMP faces significant resource pressures and called for dedicated funding for policing, prosecutions and First Nations enforcement personnel. Chief Blake urged us to make sure this bill is adequately resourced.

When I asked the RCMP whether new funding would be needed, Assistant Commissioner Ebert told us:

> I'm not sure, in relation to funding specific to this bill, how much may or may not be required . . . .

A duty without the resources to carry it out is just a promise on paper. This observation asks the government to find out what it will actually take. Funding is one piece, but even a well-funded police service needs to know the laws it's enforcing and to work with other services around it.

That brings me to the third paragraph, on coordination and training:

> In the committee's view, consideration should be given to promoting coordination among police services across Canada, including in provinces with their own police services, such as in Ontario, where the Ontario Provincial Police has jurisdiction. As well, the committee believes that such coordination could help facilitate adequate professional development and training in support of a consistent implementation of Bill S-223 across jurisdictions.

We heard that enforcement is inconsistent across the country. Assistant Commissioner Ebert told us a band in Kamloops and a band in Conne River should be treated equally.

Mr. Anderson of Manitoba Keewatinowi Okimakanak Inc., or MKO, told us, "After 30 years of non-enforcement, there is very little muscle memory on working with First Nations laws." He described sitting down with the RCMP in Manitoba to look up bylaws online. The browser the RCMP was using was so out of date, it couldn't open the *First Nations Gazette*.

> ressources et que, sans ressources suffisantes affectées au maintien de l'ordre et à l'application des lois, les communautés des Premières Nations pourraient continuer à éprouver des difficultés dans l'application de leurs lois. Le comité recommande donc vivement au gouvernement du Canada d'évaluer les ressources supplémentaires pouvant être nécessaires pour que la GRC puisse appliquer efficacement les lois des Premières Nations.

De plus, le chef Louie, du Conseil consultatif sur les terres des Premières Nations, nous a clairement dit que la GRC fait face à d'importantes contraintes en matière de ressources et a réclamé un financement dédié aux services de police, aux poursuites judiciaires et au personnel chargé de l'application de la loi au sein des Premières Nations. La cheffe de police Blake nous a exhortés à veiller à ce que le projet de loi bénéficie de ressources suffisantes.

Lorsque j'ai demandé à la GRC si un nouveau financement serait nécessaire, la commissaire adjointe Ebert nous a répondu :

> À propos des fonds nécessaires à l'application du projet de loi, je ne sais pas trop combien il faudra…

Une obligation sans les ressources nécessaires pour le remplir n'est qu'une promesse sur papier. Cette observation invite le gouvernement à déterminer ce qu'il faudra réellement. Le financement n'est qu'un élément parmi d'autres, mais même un service de police bien financé doit connaître les lois qu'il applique et collaborer avec les autres services qui l'entourent.

Cela m'amène au troisième paragraphe, qui porte sur la coordination et la formation :

> De l'avis du comité, il y aurait lieu d'envisager de promouvoir la coordination entre les services policiers au Canada, y compris dans les provinces dotées de leurs propres services de police, notamment en Ontario, où la Police provinciale de l'Ontario a compétence. Le comité est également d'avis qu'une telle coordination pourrait faciliter une formation et un développement professionnel adéquats pour assurer une mise en œuvre uniforme du projet de loi S-223 au Canada.

Nous avons entendu dire que l'application de la loi est inégale au pays. La commissaire adjointe Ebert nous a dit qu'une bande à Kamloops et une bande à Conne River devraient être traitées sur un pied d'égalité.

M. Anderson, de Manitoba Keewatinowi Okimakanak Inc., MKO, nous a déclaré : « Après 30 ans d'inaction, l'expérience pratique est très limitée en matière d'application des textes législatifs des Premières Nations. » Il a raconté s'être assis avec la GRC au Manitoba pour consulter des règlements municipaux en ligne. Le navigateur utilisé par la GRC était tellement désuet qu'il ne pouvait pas ouvrir la *Gazette des Premières Nations*.

This bill only reaches the RCMP. In Ontario, where the OPP has jurisdiction, First Nations won't see a direct benefit. This observation asks police services to work together, including on training, so that a First Nations law means the same thing no matter who polices the community.

The final paragraph in the observation picks up what may have been the clearest message we heard from every panel, which is that enforcement and prosecution go hand in hand:

> The committee further recognizes that effective enforcement of laws requires a clear path to prosecution so that the laws can be enforced, and violations of them can be prosecuted and adjudicated. Therefore, in the committee's view, without the prosecution pathway that is being proposed in Bill S-224, An Act to amend the Director of Public Prosecutions Act, the implementation of Bill S-223 may be limited.

Grand Chief Settee summed it up, saying, ". . . the basic enforcement formula is 'no enforcement without prosecution.'" The RCMP told us the same thing.

To close, I want to come back to why this matters to the communities we heard from.

Grand Chief Settee told us that during the pandemic, when First Nation leaders asked the RCMP for help enforcing their laws, " . . . they felt totally abandoned . . ."

Chief Louie asked us a simple question, ". . . how can you be a recognized government without having your laws enforced? . . ."

I fully support this bill as a strong first step toward an answer. These observations help make sure it works on the ground as well. I hope you'll join me in supporting it. Thank you.

That was a lot.

The Chair: Thank you, Senator Hay. Yes, it was. Good substance.

Before we go too much further, a couple of things: There was an opening statement, the committee notes, the committee's view and then what the committee further recognizes.

We would take a look at, as far as an observation, each of those as a package of one, just to clarify with you.

Are there any comments, questions or clarifications we are seeking from Senator Hay?

Ce projet de loi ne vise que la GRC. En Ontario, où la Police provinciale de l'Ontario, la PPO, a compétence, les Premières Nations n'en tireront aucun avantage direct. Cette observation invite les services de police à collaborer, notamment en matière de formation, afin qu'une loi de la Première Nation soit interprétée de la même manière, quel que soit le service chargé de faire respecter l'ordre dans la collectivité.

Le dernier paragraphe de cette observation reprend ce qui a sans doute été le message le plus clair que nous ayons entendu de la part de tous les groupes d'experts, à savoir que l'application de la loi et les poursuites vont de pair :

> Le comité reconnaît en outre que l'application efficace des lois doit mener à des poursuites; ainsi, les lois peuvent être appliquées et les infractions peuvent être passibles de poursuites et être jugées. Par conséquent, le comité croit qu'en l'absence du mécanisme lié aux poursuites proposé par le projet de loi S-224, Loi modifiant la Loi sur le directeur des poursuites pénales, la mise en œuvre du projet de loi S-223 pourrait être limitée.

Le grand chef Settee a résumé la situation en disant : « […] le principe fondamental en matière d'application de la loi est le suivant : "pas d'application sans poursuites" ». La GRC nous a dit la même chose.

Pour conclure, je voudrais revenir sur l'importance de cette question pour les collectivités qui se sont exprimées devant nous.

Le grand chef Settee nous a confié que pendant la pandémie, lorsque les dirigeants des Premières Nations ont demandé à la GRC de les aider à faire respecter leurs lois, « […] ils se sont sentis totalement abandonnés […] ».

Le chef Louie nous a posé une question simple : « [...] comment le gouvernement peut-il être reconnu comme tel si ses lois ne sont pas appliquées? »

J'appuie sans réserve le projet de loi, qui constitue un premier pas important vers une réponse. Ces observations contribuent à garantir qu'il fonctionne également sur le terrain. J'espère que vous vous joindrez à moi pour l'appuyer. Merci.

C'était beaucoup.

La présidente : Merci, sénatrice Hay. Oui, en effet. Un contenu de qualité.

Avant d'aller plus loin, quelques précisions : il y a eu une déclaration liminaire, les notes du comité, le point de vue du comité, puis ce que le comité reconnaît en outre.

Pour que ce soit bien clair, nous examinerions chaque observation séparément.

Souhaitons-nous obtenir des commentaires ou des précisions de la part de la sénatrice Hay ou lui poser des questions?

Senator McCallum: I want to go back to the observation, the paragraph with ". . . that Bill S-223 would confirm the Royal Canadian Mounted Police's(RCMP's) duty to enforce . . . ." It's silent.

The intent and scope of this bill regard amending the Royal Canadian Mounted Police Act. Yes, the funding did come through, but in my speech, I said that needs to be addressed differently.

Senator Hay: Yes.

Senator McCallum: When you look at all the reports done by different groups, since 2010, there have been 10 reports up to 2024, all to do with a lack of funding. There are decades of recommendations and limited government action.

This is beyond the scope of my bill, but it is within your scope, as the committee, to look at these reports and to recommend what happens. I have looked at some of them.

The Office of the Auditor General also commented on the lack of funding. It's beyond the scope of this bill, and it has been acknowledged by the government.

Senator Hay: Thank you for the clarification and also for the enormous amount of work.

My intent here regards that someone else coming into this — the government, the department — may not have the benefit of all your knowledge and research.

I wanted to attach an observation, not an amendment. I don't want to change the scope of your bill. I just want to make sure it is the obligation of the government to ensure there's funding for Bill S-223, as you point out in your research.

I am completely fine with how you want to approach it as the sponsor of this bill. If you find the observation will complicate this as it moves forward, I'm completely happy to withdraw it.

I wanted to shore up your bill and say to the Government of Canada that they are required to fund this and can't carve it out of another budget where there are limited resources as well. The RCMP doesn't have reserves of funding to earmark toward that. That was my intent, but I appreciate where you're sitting right now, senator.

Senator McCallum: Because of the bill and the scope, that it be one observation, the other one could be that the government

La sénatrice McCallum : Je voudrais revenir sur l'observation, le paragraphe qui dit « [...] que le projet de loi S-223 confirmerait l'obligation de la Gendarmerie royale du Canada (GRC) de faire respecter [...] ». Il n'y a rien à ce sujet.

L'intention et la portée de ce projet de loi concernent la modification de la Loi sur la Gendarmerie royale du Canada. Oui, le financement a bien été accordé, mais, dans mon intervention, j'ai dit que cette question devait être abordée différemment.

La sénatrice Hay : Oui.

La sénatrice McCallum : Si l'on examine tous les rapports rédigés par divers groupes depuis 2010 — il y en a eu 10 jusqu'en 2024 —, tous soulignent un manque de financement. Cela fait des décennies que des recommandations sont formulées, mais les mesures prises par le gouvernement restent limitées.

Cela dépasse la portée de mon projet de loi, mais il est de votre compétence, comme comité, d'examiner ces rapports et de formuler des recommandations sur la marche à suivre. J'en ai examiné quelques-uns.

Le Bureau de la vérificatrice générale a également fait état du manque de financement. Cela dépasse la portée de ce projet de loi, et le gouvernement l'a reconnu.

La sénatrice Hay : Merci pour cette précision et pour l'énorme travail accompli.

Mon intention ici est de souligner que d'autres intervenants — le gouvernement, le ministère — pourraient ne pas bénéficier de l'ensemble de vos connaissances et de vos recherches.

Je souhaitais ajouter une observation, et non un amendement. Je ne veux pas modifier la portée de votre projet de loi. Je veux simplement m'assurer qu'il incombe au gouvernement de garantir le financement du projet de loi S-223, comme vous le soulignez dans vos recherches.

Je souscris sans réserve à la façon dont vous souhaitez aborder la question comme marraine de ce projet de loi. Si vous estimez que cette observation risque de compliquer la suite du processus, je suis tout à fait disposée à la retirer.

Je voulais renforcer votre projet de loi et dire au gouvernement du Canada qu'il est tenu de le financer et qu'il ne peut pas prélever ces fonds d'un autre budget dont les ressources sont également limitées. La GRC ne dispose pas de réserves financières à affecter à cette fin. Telle était mon intention, mais je comprends votre position, sénatrice McCallum.

La sénatrice McCallum : Compte tenu du projet de loi et de sa portée, s'il ne doit y avoir qu'une seule observation, l'autre

needs to act on all the reports and look at how they are funding the RCMP and First Nations and Inuit policing programs.

When I met with police units across Canada, all of them said they were underfunded, including provincial policing. However, it's beyond the scope of this bill.

When you've had the Senate, the House of Commons, the Auditor General, the Management Advisory Board and the whole report — a special report on RCMP — and they haven't been able to do anything, attaching this observation will not accomplish what you would like.

I recommend that the committee investigate these reports and deal with that policing program.

Senator Hay: I completely appreciate that. I don't recall those reports being part of the committee dialogue.

Senator McCallum: No.

Senator Hay: I would withdraw my observation, and then a new observation would have to be put forward. I don't think we should delay.

I do not want the government, with all respect, to not have to consider appropriate funding for Bill S-223, as well as to the RCMP. What we know could happen is the funding side may be ignored, regardless.

If you feel this will complicate your bill as an observation, I support your bill. I support the work that's been done on it.

I'm a former banker, so I'm always worried about money.

Senator McCallum: I would like to hear what other senators think.

Senator Yussuff: I applaud Senator McCallum for bringing the bill forward, but I've been very clear that this bill will not accomplish what it set out to.

Resources are a part of the problem, but enforcing First Nation or Indigenous laws from their jurisdiction inherently has some contradictions with the Charter. This is where the RCMP has some challenges in their dilemma and responsibilities. How do they enforce laws that are not necessarily from their thinking? It is their training and responsibility.

pourrait être que le gouvernement doit donner suite à tous les rapports et examiner le financement qu'il accorde à la GRC ainsi qu'aux services de police des Premières Nations et des Inuits.

Lorsque j'ai rencontré des représentants de services de police partout au Canada, tous m'ont dit qu'ils manquaient de fonds, y compris les corps de police provinciaux. Cependant, cela dépasse la portée de ce projet de loi.

Quand on a eu le Sénat, la Chambre des communes, la vérificatrice générale, le Conseil consultatif de gestion et le rapport dans son ensemble — un rapport spécial sur la GRC — et qu'ils n'ont rien pu faire, ajouter cette observation ne permettra pas d'atteindre votre objectif.

Je recommande que le comité examine ces rapports et se penche sur ce programme de services de police.

La sénatrice Hay : Je suis tout à fait d'accord. Je ne me souviens pas que ces rapports aient fait partie des discussions du comité.

La sénatrice McCallum : Non.

La sénatrice Hay : Je retirerais alors mon observation, et une nouvelle observation devrait être présentée. Je ne pense pas que nous devrions retarder les choses.

Avec tout le respect que je vous dois, je ne veux pas que le gouvernement soit dispensé d'envisager un financement adéquat pour le projet de loi S-223, ainsi que pour la GRC. Ce qui risque d'arriver, c'est que l'aspect financier soit ignoré, quoi qu'il arrive.

Si vous estimez que cette observation compliquera votre projet de loi, je soutiens votre projet de loi. Je soutiens le travail qui a été accompli à cet égard.

J'étais banquière dans une autre vie, donc je me soucie toujours des questions d'argent.

La sénatrice McCallum : J'aimerais entendre ce qu'en pensent les autres sénateurs.

Le sénateur Yussuff : Je félicite la sénatrice McCallum d'avoir présenté le projet de loi, mais j'ai clairement dit que celui-ci n'atteindra pas les objectifs qu'il s'est fixés.

Les ressources font partie du problème, mais l'application des lois des Premières Nations ou du droit autochtone relevant de leur compétence comporte intrinsèquement certaines contradictions avec la Charte. C'est là que la GRC se retrouve confrontée à des défis liés à son dilemme et à ses responsabilités. Comment peut-elle faire respecter des lois qui ne correspondent pas nécessairement à sa propre vision? Cela relève de sa formation et de ses responsabilités.

The bigger challenge will be when the bill goes to the other place, where I think it will receive far more scrutiny than on this side of Parliament. It will go through a different level of rigour. That's for the other place to determine.

I think Senator Hay's observation was trying to highlight what we have heard as a way to provide some appreciation for the other place. However, what those paragraphs highlight will turn this bill into something requiring a Royal Recommendation because you are asking the government to spend money on a private member's bill that is problematic in a general context for a private member's bill.

I understand what the bill is attempting to do. I don't think it will accomplish that from what I heard from the RCMP and given the history of the country. With that aside, if it passes through the chamber, it will go to the other place. We will let them figure out what they want to do with the bill because that's their jurisdiction and responsibility.

I see this in a problematic way. I say that candidly because I don't think it will accomplish what it set out to accomplish; that's my observation from hearing the witnesses who came before us from the RCMP, because, ultimately, they are the ones who are on the front line having to carry out the responsibility of enforcing First Nations laws. There are some inherent contradictions with their understanding. They know Canadian laws because they are trained to, and they work with the prosecution service. The other side is that the prosecution service at the provincial level is not yet versed on how to enforce First Nations laws.

The Chair: Senator Hay, as you listened and spoke, great work. Are you open to moving forward with these observations? Are you feeling as if you wish to pull them? I have no opinion. I am asking the question.

Senator Hay: Thank you for that. If I could ask the indulgence of the committee, I would love to hear your feedback.

I will withdraw the observation because I'm respectful of your commentary, Senator McCallum. Thank you for that clarity. This is great learning for me.

I would love to hear what you were going to say, Senator Pate and Senator Cardozo.

The Chair: Absolutely. Thank you for that.

Senator Pate: If you didn't withdraw it, one suggestion I thought might capture some of what's been discussed is to delete the first sentence. Then, with the second sentence, the observation would be, "The committee heard that the RCMP already faces significant resource pressures . . . ."

Le plus grand défi se posera lorsque le projet de loi sera renvoyé à l'autre endroit, où je pense qu'il fera l'objet d'un examen bien plus minutieux qu'ici. Il sera soumis à un niveau de rigueur différent. C'est à l'autre endroit d'en décider.

Je crois que l'observation de la sénatrice Hay visait à mettre en lumière ce que nous avons entendu afin de susciter une certaine reconnaissance de la part de l'autre endroit. Cependant, ce que ces paragraphes mettent en lumière fera de ce projet de loi un texte nécessitant une recommandation royale, car vous demandez au gouvernement de consacrer des fonds à un projet de loi d'initiative parlementaire qui pose un problème dans le contexte général de ce type de projet de loi.

Je comprends ce que le projet de loi tente de faire. Je ne pense pas qu'il y parviendra, d'après ce que j'ai entendu de la GRC et compte tenu de l'histoire du pays. Cela dit, s'il est adopté au Sénat, il sera renvoyé à l'autre endroit. Nous les laisserons décider de ce qu'ils veulent faire de ce projet de loi, car cela relève de leur compétence et de leur responsabilité.

Je vois cela d'un œil critique. Je le dis en toute franchise, car je ne pense pas qu'il atteindra l'objectif qu'il s'est fixé; c'est ce que je retiens après avoir entendu les témoins de la GRC qui ont comparu devant nous, car, en fin de compte, ce sont eux qui sont en première ligne et qui doivent assumer la responsabilité de faire respecter les lois des Premières Nations. Il existe certaines contradictions inhérentes à leur compréhension. Ils connaissent les lois canadiennes, car ils ont reçu une formation à cet effet, et ils travaillent avec le service des poursuites. Par ailleurs, le service des poursuites à l'échelle provinciale ne maîtrise pas encore la manière d'appliquer les lois des Premières Nations.

La présidente : Sénatrice Hay, bravo pour votre écoute et vos interventions. Êtes-vous disposée à aller de l'avant avec ces observations? Souhaitez-vous plutôt les retirer? Je n'ai pas d'opinion à ce sujet. Je vous pose simplement la question.

La sénatrice Hay : Merci. Si le comité me le permet, j'aimerais beaucoup connaître votre avis.

Je vais retirer cette observation, car je respecte votre remarque, sénatrice McCallum. Merci pour cette précision. C'est très instructif pour moi.

J'aimerais beaucoup entendre ce que vous alliez dire, sénatrice Pate et sénateur Cardozo.

La présidente : Bien sûr. Merci.

La sénatrice Pate : Si vous ne l'aviez pas retirée, une suggestion qui, selon moi, pourrait refléter en partie la discussion serait de supprimer la première phrase. Ensuite, en reprenant la deuxième phrase, l'observation serait : « Le comité a entendu que la GRC doit déjà faire face à des contraintes importantes en matière de ressources [...] ».

Then take out the next phrase, and then:

> . . . and that First Nation communities could continue to experience challenges in the enforcement of their laws. The committee therefore strongly encourages the Government of Canada to address countless reports recommending additional resources be provided, so that the RCMP can enforce First Nation laws effectively.

I think that gets at your intent without going into the scope of the bill, but it pushes the government to look at the resource issue and references that there are previous reports that have recommended that.

I defer to you on whether that meets the concern or whether you would rather see it withdrawn.

Senator McCallum: I would rather see it withdrawn.

Senator Cardozo: I also want to add my compliments to Senator McCallum for all the work you have done on this bill and bringing it forward.

As I went through the process, the part where the penny dropped for me was when it was explained, or at least the way I understood it, that it's not that different from the RCMP enforcing bylaws of municipalities across the country. That's how I saw the RCMP witnesses seeing it. I see it as fairly straightforward in that context.

I like the intent and what Senator Hay laid out. As you say, if it is complicating matters, I'm happy not to go with it. The main thing is that we move the bill along. It's gone through a lot of work, and I'm happy to support it moving ahead.

Senator McCallum: I wanted to address the Charter.

In the Lands Advisory Board, or LAB, submission, they said:

> First Nation law making authority should be clarified in all legislation governing police forces, so police officers have no doubts as to their authority to assist First Nation police services or exercise their authority when called upon to do so. Not only should police authority be crystal clear but standard protections and limitations of liability for police officers must also be crystal clear . . .

Ensuite, retirez la phrase suivante, puis :

> [...] et que les communautés des Premières Nations pourraient continuer à éprouver des difficultés dans l'application de leurs lois. Le comité recommande donc vivement au gouvernement du Canada d'évaluer les ressources supplémentaires pouvant être nécessaires pour que la GRC puisse appliquer efficacement les lois des Premières Nations.

Je pense que cela reflète votre intention sans modifier la portée du projet de loi, mais que cela incite le gouvernement à se pencher sur les ressources et fait mention des rapports antérieurs qui ont formulé cette recommandation.

Je m'en remets à vous pour déterminer si cela répond à votre préoccupation ou si vous préférez que cette proposition soit retirée.

La sénatrice McCallum : Je préférerais que cette proposition soit retirée.

Le sénateur Cardozo : Je tiens également à féliciter la sénatrice McCallum pour tout le travail qu'elle a accompli sur le projet de loi et pour l'avoir présenté.

Au cours de ce processus, j'ai eu une révélation lorsqu'on m'a expliqué — ou du moins, c'est ainsi que je l'ai compris — que cela n'était pas si différent de l'application par la GRC des règlements municipaux partout au pays. C'est ainsi que j'ai perçu le point de vue des témoins de la GRC. Je trouve cela assez simple dans ce contexte.

J'aime l'intention et ce que la sénatrice Hay a exposé. Comme vous dites, si cela complique les choses, je suis disposé à ne pas l'inclure. L'essentiel est de faire avancer le projet de loi. Il a fait l'objet d'un travail considérable, et je suis heureux d'appuyer sa progression.

La sénatrice McCallum : Je voulais aborder la question de la Charte.

Dans le mémoire du Conseil consultatif des terres, le CCT, on dit :

> Le pouvoir législatif des Premières Nations devrait être clarifié dans toutes les lois régissant les forces de police, de sorte que les agents de police n'aient aucun doute quant à leur pouvoir d'appuyer les services de police des Premières Nations ou d'exercer leur autorité lorsqu'ils sont appelés à le faire. Les pouvoirs de la police doivent être absolument clairs, tout comme les protections normales et les limitations de responsabilité des agents de police [...].

The continue, saying that this legislation, Bill S-223:

> . . . clarify legal authority and provide all standard protections is vital, as RCMP and prosecutors are routinely advised by their lawyers that they do not have what they need to enforce . . . . .

However, this bill will give standard protection and limitation of liability for police officers because, as Senator Cardozo said, municipal, city and every law is enacted. The only other ones are First Nations, and that is a Charter breach. Why are they the only ones?

The Chair: Any other thoughts or comments at this moment?

Senator Hay: Thank you, all, for my learning opportunity tonight and also for the good dialogue. It was great.

Thank you, Senator McCallum.

The Chair: The learning is every day until you're not doing this any longer.

It is agreed then, to be clear, there will be no amendments coming forward.

I would ask then to report this bill to the Senate in both official languages.

Hon. Senators: Agreed.

(The committee continued in camera.)

Au sujet de ce projet de loi, le projet de loi S-223, le CCT poursuit :

> [...] Il est essentiel de préciser dans la loi quels sont les pouvoirs légaux et de fournir toutes les protections normales, car la GRC et les procureurs sont régulièrement avisés par leurs avocats qu'ils n'ont pas ce qu'il faut pour appliquer les lois [...].

Cependant, ce projet de loi accordera une protection normale et limitera la responsabilité des agents de police parce que, comme l'a dit le sénateur Cardozo, les lois municipales et autres sont promulguées. Les seules autres concernent les Premières Nations, ce qui constitue une violation de la Charte. Pourquoi sont-elles les seules?

La présidente : Y a-t-il d'autres réflexions ou observations pour le moment?

La sénatrice Hay : Merci à tous pour cette occasion d'en apprendre davantage ce soir, ainsi que pour ce fructueux échange. Ce fut formidable.

Merci, sénatrice McCallum.

La présidente : On apprend tous les jours, jusqu'à ce qu'on cesse d'exercer cette fonction.

Il est donc convenu, pour que ce soit clair, qu'aucun amendement ne sera proposé.

Je demande donc que rapport soit fait de ce projet de loi au Sénat dans les deux langues officielles.

Des voix : D'accord.

(La séance se poursuit à huis clos.)