## EVIDENCE

OTTAWA, Monday, November 18, 2024

The Standing Senate Committee on National Security, Defence and Veterans Affairs met with videoconference this day at 4 p.m. [ET] to study Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts; and to examine and report on issues relating to national security and defence generally.

**Senator Hassan Yussuff** (*Chair*) in the chair.

[*English*]

**The Chair:** Good afternoon, senators. Before I begin, I would like to ask all senators and other persons in the room to consult the cards on the table for guidelines to prevent audio feedback incidents. You may see a little thing right beside you there, so if you can refer to that, it will be helpful.

Welcome this meeting of the Standing Senate Committee on National Security, Defence and Veterans Affairs. I'm Hassan Yussuff. I'm from Ontario and the chair of the committee. I am joined today by my fellow committee members, who will introduce themselves starting on my right with our colleague and deputy chair.

[*Translation*]

**Senator Dagenais:** Jean-Guy Dagenais from Quebec.

[*English*]

**Senator Richards:** Dave Richards, New Brunswick.

**Senator M. Deacon:** Welcome. Marty Deacon, Ontario.

**Senator McNair:** John McNair, New Brunswick.

**Senator Ross:** Krista Ross, New Brunswick.

**Senator Dasko:** Donna Dasko from Ontario.

**Senator LaBoucane-Benson:** Welcome. Patti LaBoucane-Benson, Treaty 6 Territory, Alberta.

**Senator Kutcher:** Stan Kutcher, Nova Scotia.

**Senator Cardozo:** Andrew Cardozo from Ontario. Mr. Chair, I look forward to your first meeting as chair. Congratulations.

## TÉMOIGNAGES

OTTAWA, le lundi 18 novembre 2024

Le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants se réunit aujourd'hui, à 16 heures (HE), avec vidéoconférence, pour étudier le projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois; et afin d'examiner, pour en faire rapport, les questions concernant la sécurité nationale et la défense en général.

**Le sénateur Hassan Yussuff** (*président*) occupe le fauteuil.

[*Traduction*]

**Le président :** Bon après-midi, chers collègues. Avant de commencer, j'invite les sénatrices et les sénateurs ainsi que tous les autres participants sur place à consulter les fiches disposées sur la table pour prendre connaissance des directives à respecter pour prévenir les incidents de rétroaction acoustique. Elles devraient être facilement accessibles, donc je vous prie de vous y référer.

Bienvenue à cette séance du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Je m'appelle Hassan Yussuff. Je viens de l'Ontario et je préside le comité. Je suis accompagné aujourd'hui de mes collègues du comité, que j'invite à se présenter, en commençant par le vice-président, à ma droite.

[*Français*]

**Le sénateur Dagenais :** Jean-Guy Dagenais, du Québec.

[*Traduction*]

**Le sénateur Richards :** Dave Richards, du Nouveau-Brunswick.

**La sénatrice M. Deacon :** Bienvenue. Marty Deacon, de l'Ontario.

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

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

**La sénatrice Dasko :** Donna Dasko, de l'Ontario.

**La sénatrice LaBoucane-Benson :** Bienvenue. Patti LaBoucane-Benson, du territoire du Traité nº 6, de l'Alberta.

**Le sénateur Kutcher :** Stan Kutcher, de la Nouvelle-Écosse.

**Le sénateur Cardozo :** Andrew Cardozo, de l'Ontario. Monsieur le président, j'attends avec impatience que commence votre première séance en tant que président. Félicitations.

**The Chair:** Thank you. I have the gavel.

Today we continue our consideration of Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

We will hear from these three panels of witnesses who will share their insight on this bill. In the first panel, I'm pleased to welcome in the room today with us, David Shipley, Chief Executive Officer and Co-Founder, Beauceron Security Inc.; Todd Warnell, Chief Information Security Officer, Bruce Power; and Sharon Polsky, President, Privacy and Access Council of Canada.

Thank you very much for joining us today. We invite you to provide opening remarks to be followed by questions from our members. I remind you that each of you will have five minutes to present. We'll begin today's presentation with Mr. David Shipley. Please proceed when you're ready.

**David Shipley, Chief Executive Officer and co-founder, Beauceron Security Inc.:** Thank you so much. I appreciate the opportunity to be here today.

My name is David Shipley, and I am the chief executive officer and co-founder of Beauceron Security Inc. I am also a co-chair of the Canadian Chamber of Commerce's cyber council.

Beauceron Security works with global banks, national telecommunications companies, provincial and municipal governments, higher education and more, helping educate and motivate individuals to make good decisions about technology so they can reduce their cyber risk and thrive in a digital world. We serve more than 1,090 clients, primarily in Canada but also in the United States, Europe and Africa.

I support the need for this legislation. We need this now more than ever. We're far behind our allies, and we're risking the safety and prosperity of Canadians every day that we delay.

I draw your attention to April 2023 when we learned through a U.S. intelligence leak that a Canadian pipeline provider was hacked by the Russian hacking group Zarya. Zarya's intent was to cause economic damage, and its attack could also have risked human life. Here we are, a year and a half later, still working through the laws that we hope someday will reduce this risk.

**Le président :** Merci. En effet, c'est moi qui ai le marteau.

Aujourd'hui, nous poursuivons notre étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Nous allons entendre trois groupes de témoins qui nous présenteront leur point de vue sur le projet de loi. J'ai le plaisir d'accueillir, dans le premier groupe de témoins, tous ici présents, David Shipley, chef de la direction et cofondateur, Beauceron Security Inc.; Todd Warnell, directeur de la sécurité de l'information, Bruce Power; et Sharon Polsky, présidente, Conseil du Canada de l'accès et la vie privée.

Merci à vous tous de vous joindre à nous, aujourd'hui. Nous vous invitons maintenant à faire votre déclaration préliminaire, qui sera suivie des questions des membres du comité. Je vous rappelle que vous avez chacun cinq minutes pour faire votre déclaration. Nous allons commencer par M. David Shipley. Veuillez commencer dès que vous serez prêt.

**David Shipley, chef de la direction et cofondateur, Beauceron Security Inc. :** Merci beaucoup. Je suis très content d'être ici.

Je m'appelle David Shipley, et je suis le chef de la direction et le cofondateur de Beauceron Security Inc. Je suis également coprésident du conseil de cybersécurité de la Chambre de commerce du Canada.

Beauceron Security travaille avec des banques mondiales, des entreprises de télécommunications nationales, des gouvernements provinciaux, des administrations municipales, des établissements d'éducation supérieure et bien d'autres entités, afin d'éduquer les gens et de les encourager à prendre de bonnes décisions en matière de technologie afin de réduire leurs risques de cybersécurité et de pouvoir s'épanouir dans un monde numérique. Nous aidons plus de 1 090 clients, principalement au Canada, mais également aux États-Unis, en Europe et en Afrique.

Je crois, moi aussi, que le projet de loi est nécessaire. Cela n'a jamais été autant nécessaire. Nous sommes loin derrière nos alliés, et nous risquons la sécurité et la prospérité des Canadiens chaque jour où nous tardons à l'adopter.

J'aimerais vous rappeler que, en avril 2023, nous avons découvert, grâce à une fuite de renseignement américain, qu'un groupe de cyberpirates russes, Zarya, avait attaqué un fournisseur de pipelines. Zarya voulait causer des dommages économiques, et son attaque aurait également pu mettre en péril des vies humaines. Nous voici, un an et demi plus tard, toujours en train de travailler sur des lois qui, nous l'espérons, réduiront un jour ce risque.

I was recently informed there were other attacks on Canadian critical infrastructure that did not garner attention that could have posed safety risks.

I want to acknowledge that important changes I, my colleagues on the cyber council and others advocated during parliamentary hearings and have been reflected. The deletion of clause 10 and subsequent restoration of the due diligence defence, the removal of the requirement for immediate reporting of cybersecurity incidents and the harmonization with existing obligations in North America were all needed changes.

I do believe there are more changes that could be made to this bill to ensure that it serves its purpose best, although I'm cautious that any amendment process could potentially jeopardize the bill passing in a timely fashion. However, it is worth noting that the proposed addition in Part 1, clause 6, no compensation, to the Telecommunications Act should be considered for an amendment to look at compensation for telecommunications service providers under the following circumstances. For example, if an order required a change of a technology vendor at immediate cost to the business without the ability of the organization to phase out the technology or service in a planned fashion in accordance with their technology life cycle plans or over a period of multiple years so that changes can be budgeted and accounted for so they can be entitled to some compensation, particularly when thinking of regional service providers who don't have the wallets to do these kinds of changes at a moment's notice.

The sections of the law that deal with individual liability remain hugely problematic. I can personally attest to several senior cybersecurity leaders, specifically chief information security officers, in critical infrastructure who have indicated they intend to quit their jobs if the law passes at it stands, which will only serve to make things more dangerous in our critical infrastructure sectors. The number of experienced cybersecurity leaders looking to leave the field due to stress and burnout is already at crisis levels, with nearly half looking to leave the role.

I believe individual liability, if it is to be maintained in the law, should solely be limited to directors of a corporation as this is the group charged with setting the risk appetite, ensuring governance structures and ensuring resources required to comply with the law.

The importance of two-way information sharing. As it stands, the legislation only contemplates one-way reporting, and it remains is a huge missed opportunity.

J'ai récemment appris qu'il y avait eu d'autres attaques contre l'infrastructure critique du Canada, qui sont passées sous silence, et qui auraient pu présenter des risques en matière de sûreté.

J'aimerais reconnaître que d'importants changements proposés, par moi-même, mes collègues du conseil de la cybersécurité et d'autres personnes pendant les séances parlementaires, ont été acceptés. La suppression de l'article 10 et le rétablissement subséquent de la défense de diligence raisonnable, le retrait de l'obligation de signaler immédiatement des incidents de cybersécurité et l'harmonisation avec les obligations existantes en Amérique du Nord étaient tous des changements nécessaires.

Je crois que, pour que le projet de loi atteigne ses objectifs, d'autres changements devraient être apportés, mais je sais qu'un quelconque processus d'amendement pourrait retarder l'adoption du projet de loi. Toutefois, il est important de noter que l'ajout proposé à l'article 6 de la partie 1 de la Loi sur les télécommunications, intitulé Aucune indemnité, devrait être amendé et qu'il faudrait examiner les indemnités pour les fournisseurs de services de télécommunications dans les cas suivants. Par exemple, si un décret imposé à une entreprise de changer à ses frais de fournisseur de technologie, sans lui donner la possibilité d'abandonner progressivement la technologie ou le service, en suivant un plan, et en respectant le cycle de vie de la technologie, ou à le faire sur multiples années afin de pouvoir budgéter les changements pour avoir droit à certaines indemnités, et je pense en particulier aux fournisseurs de service régionaux qui n'ont pas assez d'argent pour faire ce genre de changements sans préavis.

Les articles de la loi qui concernent la responsabilité personnelle demeurent extrêmement problématiques. J'ai personnellement constaté que plusieurs hauts dirigeants en cybersécurité, en particulier les dirigeants principaux de la sécurité de l'information, dans l'infrastructure critique, ont dit qu'ils allaient démissionner si la loi était adoptée telle quelle, ce qui ne peut que faire augmenter les risques dans nos secteurs d'infrastructure critiques. Nous faisons déjà face à une crise, puisque de nombreux hauts dirigeants chevronnés, soit presque la moitié, envisagent de quitter le domaine en raison du stress et de l'épuisement professionnel.

Je crois que la responsabilité personnelle, si elle reste dans la loi, devrait uniquement s'appliquer aux administrateurs de la société, puisque ce sont eux qui déterminent l'appétit pour le risque, établissent les structures de gouvernance et réunissent les ressources nécessaires pour respecter la loi.

La communication bidirectionnelle est également importante. Actuellement, le projet de loi envisage seulement le signalement dans une direction, et cela reste une belle occasion manquée.

I would be remiss if I didn't take the opportunity to point out that while I strongly support the need for this legislation, it represents the bare minimum legislatively that the federal government can do to help protect Canadians.

By focusing Bill C-26 on federally regulated sectors in telecommunications, financial services, energy transmission and transportation, the government focused on federal responsibility over national security in the broadest sense. These sectors are already the best resourced and best defended in the country.

This law does nothing to protect our health care system, which has borne the brunt of repeated major disruptive attacks, such as what happened in Newfoundland and more recently in Ontario. These attacks go beyond terrible impacts on privacy, such as the leak of reproductive health choices or nude images of people battling various cancers, they can have life-threatening impacts as has been recently stated by the head of the World Health Organization and in recent U.S. research on health care ransomware attacks.

Our increasingly high-tech agricultural sector, which now has fully automated smart tractors that are vulnerable to severe disruption, remains without a proper strategy or focus.

Nor does this law help Canadian small businesses and everyday citizens who are suffering from an increasing plague of AI-powered cyber fraud.

These are but three glaring examples of the growing national threats due to cybersecurity at a time when the federal government has still yet to publicly announce its updated strategy from 2018.

I urge the Senate to publicly study the ransomware plague, the crisis in health care cybersecurity and the future national security implications of an increasingly hostile digital world.

I look forward to discussing Bill C-26 with you further and answering what questions you may have for me. Thank you.

**The Chair:** Thank you, Mr. Shipley.

**Todd Warnell, Chief Information Security Officer, Bruce Power:** Thank you, Mr. Chair and members of the committee. My name is Todd Warnell, and I am the chief information security officer at Bruce Power.

Established in 2001, Bruce Power is Canada's only private sector nuclear generator, annually producing about one third of Ontario's power and life-saving medical isotopes used globally

Je m'en voudrais de ne pas en profiter pour dire que, même si je crois fermement que le projet de loi est nécessaire, il demeure le strict minimum que peut faire le gouvernement fédéral pour protéger les Canadiens.

Le gouvernement, en axant le projet de loi C-26 sur les secteurs des télécommunications, des services financiers, de la transmission énergétique et des transports, qui sont réglementés par le gouvernement fédéral, a mis l'accent sur la responsabilité fédérale plutôt que sur la sécurité nationale dans son ensemble. Ces secteurs jouissent déjà des meilleures ressources et de la meilleure protection au pays.

La loi ne protège pas notre système de soins de santé, qui a subi à répétition la majorité des attaques dévastatrices, par exemple à Terre-Neuve et, plus récemment, en Ontario. Ces attaques n'ont pas seulement d'énormes répercussions sur la confidentialité, comme la publication des choix en matière de santé reproductive ou d'images de personnes nues qui luttent contre divers cancers; elles peuvent également, selon la direction de l'Organisation mondiale de la santé et de récentes recherches américaines sur les attaques de rançongiciels contre le secteur de la santé, mettre en péril la vie des gens.

Notre secteur agricole, de plus en plus à la fine pointe de la technologie, utilise aujourd'hui des tracteurs intelligents entièrement automatisés qui risquent d'être la cible de graves perturbations, et n'a toujours pas adopté une stratégie adéquate ni défini d'objectif pour ce secteur.

La loi n'aide pas non plus les petites entreprises canadiennes et les citoyens victimes de l'épidémie grandissante de fraudes informatiques soutenues par l'IA.

Ce sont seulement trois exemples frappants de la menace nationale grandissante à la cybersécurité, alors que le gouvernement fédéral n'a toujours pas annoncé publiquement la mise à jour de sa stratégie de 2018.

J'implore le Sénat d'étudier publiquement l'épidémie de rançongiciels, la crise de la cybersécurité du secteur de la santé et les conséquences à venir sur la sécurité nationale d'un environnement numérique de plus en plus hostile.

J'ai bien hâte de discuter davantage avec vous du projet de loi C-26 et de répondre à vos questions. Je vous remercie.

**Le président :** Merci, monsieur Shipley.

**Todd Warnell, directeur de la sécurité de l'information, Bruce Power :** Merci, monsieur le président et merci à tous les membres du comité. Je m'appelle Todd Warnell, et je suis le directeur de la sécurité de l'information de Bruce Power.

L'entreprise Bruce Power, qui a été fondée en 2001, est le seul exploitant de centrale nucléaire du secteur privé, au Canada, et elle produit environ un tiers de l'énergie de l'Ontario et des

to fight cancer around the world and sterilize medical equipment globally.

I am grateful for the invitation to participate in your review of Bill C-26. Today, I will focus my comments on the imperative need for proceeding with the implementation of this legislation, particularly Part 2 of the bill, namely the critical cyber systems protection act, or CCSPA.

Bill C-26 represents a pivotal first step in fortifying the resilience and security of Canada's critical infrastructure to ensure the safety, reliability and integrity of essential services for all Canadians. This legislation is not merely a policy proposal but a commitment to safeguarding the backbone of our nation's economy and security in an increasingly complex and evolving global cyber threat landscape.

Within Canada's nuclear industry, we have demonstrated that through collaboration with government, regulators, industry, academia and individual Canadians, we can successfully establish and regulate cyber systems that are crucial to the safe and reliable operation of critical services.

Bill C-26 aims to secure essential systems, encourage proactive risk management and enable responsible government intervention in cases of significant cyber-threats. The critical cyber systems protection act will introduce a broad framework from which all critical sectors in collaboration with government and regulators can develop and implement risk-informed and performance-based regulations to enhance the reliability and resilience of critical services.

There are several key benefits to proceeding with Bill C-26. Namely, strengthening national security and safety. Bill C-26 is crucial for protecting national security by requiring both private and public organizations within critical infrastructure sectors to adopt robust cybersecurity practices. As cyber-threats evolve and become more sophisticated, securing critical infrastructure and services is paramount to maintaining national security and public safety.

Enhanced risk management. By enforcing mandatory risk management practices, the bill helps organizations move away from a reactive posture to a proactive approach that minimizes risks before they escalate into actual incidents.

Government authority in high-risk scenarios. The bill empowers government authorities to intervene in critical infrastructure during severe threats. This capability is crucial for responding swiftly to imminent attacks or breaches, preventing

isotopes médicaux vitaux utilisés mondialement pour combattre le cancer et désinfecter les équipements médicaux.

Je suis heureux d'avoir été invité à participer à votre étude du projet de loi C-26. Aujourd'hui, je vais insister sur le besoin impératif d'adopter le projet de loi, et en particulier la partie 2 du projet de loi, à savoir la Loi sur la protection des cybersystèmes essentiels.

Le projet de loi C-26 est une première étape importante vers le renforcement de la résilience et de la sécurité des infrastructures canadiennes essentielles pour assurer la sécurité, la fiabilité et l'intégrité des services essentiels pour tous les Canadiens. Ce n'est pas une simple proposition, c'est un engagement à protéger l'épine dorsale de l'économie et la sécurité de la nation, dans un environnement de menace de cybersécurité mondiale de plus en plus complexe et en constante évolution.

Dans l'industrie nucléaire canadienne, nous avons montré que, grâce à la collaboration avec le gouvernement, les organismes de réglementation, les universitaires et tous les Canadiens, nous sommes capables de mettre sur pied et de réglementer les systèmes de cybersécurité qui sont nécessaires au fonctionnement sécuritaire et fiable des services essentiels.

L'objectif du projet de loi C-26 est de sécuriser les systèmes essentiels, d'encourager la gestion proactive du risque et d'assurer une intervention responsable du gouvernement en cas de cybermenaces importantes. La Loi sur la protection des cybersystèmes essentiels établit un cadre général à partir duquel tous les secteurs essentiels, aux côtés du gouvernement et des organismes de réglementation, peuvent élaborer et mettre en œuvre des règlements fondés sur le risque et sur le rendement pour assurer la fiabilité et la résilience des services essentiels.

L'adoption du projet de loi C-26 se traduit par plusieurs avantages, et surtout par le renforcement de la sécurité et de la sûreté nationale. Le projet de loi C-26 est essentiel à la protection de la sécurité nationale parce qu'il oblige les organismes privés et publics œuvrant dans les secteurs des infrastructures critiques à respecter de solides pratiques en matière de cybersécurité. Alors que les cybermenaces continuent d'évoluer et de se perfectionner, il est essentiel d'assurer la sécurité dans l'infrastructure et des services afin de maintenir la sécurité nationale et la sécurité du public.

Une meilleure gestion des risques. Le projet de loi, en obligeant l'adoption de pratiques de gestion des risques, aide les organisations à délaisser leur position réactive en faveur d'une approche proactive, qui réduit au minimum les risques avant qu'ils ne deviennent des incidents réels.

Les autorités du gouvernement dans les situations à risque élevé. Le projet de loi permet aux autorités gouvernementales d'intervenir dans l'infrastructure critique en cas de menaces graves. Ce pouvoir essentiel lui permet de réagir rapidement aux

or minimizing potential damage to essential services, and maintaining public trust.

Alignment with global allies. Our allies are implementing or strengthening similar cybersecurity laws in their nations. Bill C-26 allows Canada to align with international partners and makes it easier for Canadian companies to operate globally within secure and trusted frameworks.

Finally, economic security. Cyberattacks on critical sectors can have far-reaching economic implications. By ensuring key industries and services are protected, Canada also safeguards its economic stability, helping prevent the cascading consequences that could arise from disrupted infrastructure.

In conclusion, Bill C-26 is a well-intentioned first step to address the pressing issue of cybersecurity in Canada's critical infrastructure sectors. Thank you for the opportunity to address the committee, and I look forward to your questions today.

**The Chair:** Thank you, Mr. Warnell.

**Sharon Polsky, President, Privacy and Access Council of Canada:** Thank you so much for the invitation to address the committee today. I'm Sharon Polsky, president of the Privacy and Access Council of Canada, or PACC, an independent, non-profit, non-partisan organization that is not funded by government or industry.

Since its launch more than 30 years ago, the internet has become an integral part of our everyday lives. It enables research, commerce, communication and democratic freedoms. The internet also facilitates harmful conduct such as harassment, ransom demands, hostile activities by unfriendly states — all sorts of behaviours that existed long before the internet enabled such abhorrent activity to be carried out with great ease and broad reach.

Bill C-26 is one of several bills advanced by Canada's government to protect Canadians from such harms, but it also illustrates how proposed cures can be worse than the disease itself. In the name of strengthening cybersecurity, the bill grants the government sweeping power to order telecommunication providers — the very same telecoms that are now the repositories of our most intimate, sensitive and health-related data — ". . . to do a specified thing or refrain from doing a specified thing . . . ." Similar powers, of course, apply to operators designated under Part 2 of the bill.

attaques imminentes ou aux fuites, afin de prévenir ou de réduire au minimum les dommages possibles aux services essentiels et de conserver la confiance du public.

S'harmoniser avec nos alliés mondiaux. Chez eux, nos alliés mettent en œuvre ou améliorent des lois semblables en matière de cybersécurité. Le projet de loi C-26 permet au Canada de s'harmoniser avec ses partenaires internationaux et aux entreprises canadiennes de mener plus facilement leurs activités partout dans le monde, à l'intérieur de cadres sûrs et éprouvés.

Pour finir, il y a la sécurité économique. Les cyberattaques contre les secteurs essentiels peuvent avoir des répercussions considérables sur l'économie. Le Canada, en assurant la protection des industries et des services clés, protège également sa stabilité économique, et permet d'éviter les conséquences en cascades d'une perturbation de l'infrastructure.

En conclusion, le projet de loi C-26 est une première étape bien intentionnée si l'on veut régler la question urgente de la cybersécurité des secteurs de l'infrastructure critiques du Canada. Merci de m'avoir invité à discuter avec le comité, et j'ai bien hâte d'entendre vos questions.

**Le président :** Merci, monsieur Warnell.

**Sharon Polsky, présidente, Conseil du Canada de l'accès et la vie privée :** Merci beaucoup de m'avoir invitée à comparaître devant le comité, aujourd'hui. Je m'appelle Sharon Polsky, et je suis présidente du Conseil du Canada de l'accès et la vie privée, un organisme indépendant et sans but lucratif qui n'est pas financé par le gouvernement ni par l'industrie.

Depuis son lancement, il y a de ça plus de 30 ans, Internet est devenu partie intégrante de notre quotidien. Internet nous offre la liberté en matière de recherche, d'échanges commerciaux, de communication et de démocratie. Internet facilite également les comportements préjudiciables, comme le harcèlement, les demandes de rançon, les activités hostiles d'États ennemis, toutes sortes de comportements qui existaient bien avant qu'Internet ne permette à ce genre d'activités odieuses de se faire plus facilement et d'atteindre un grand nombre de personnes.

Le projet de loi C-26 est l'un des multiples projets de loi proposés par le gouvernement canadien afin de protéger les Canadiens de tels préjudices, mais il montre également que le remède peut être pire que le mal. Afin de renforcer la cybersécurité, le projet de loi accorde un pouvoir très étendu au gouvernement, qui peut ordonner aux fournisseurs des services de télécommunications — ceux-là mêmes qui stockent nos données de santé les plus intimes et les plus délicates — « ... de faire ou de s'abstenir de faire toute chose qu'il précise... » Bien sûr, des pouvoirs semblables sont accordés aux exploitants définis à la partie 2 du projet de loi.

Bill C-26's omission of vital democratic checks and balances to constrain such alarmingly broad powers rightfully sparked an avalanche of criticism, because this is not a zero-sum game. I think we can all agree on the need for cybersecurity, but not when it's at the cost of our civil liberties. I do want to acknowledge the work of members in the other place in curbing some of this bill's most egregious excesses, but even with that, Bill C-26 contains significant flaws that risk-compromising civil liberties and cybersecurity. Let me give you a few practical examples.

First, Bill C-26 gives the government the power to order telecommunication providers to adopt standards that actually weaken encryption and privacy with it. This endangers the freedom of everyone in Canada, including political representatives, to safely engage in national and international commerce and communications and enjoy private communications.

Second, Bill C-26 allows the government to indefinitely keep secret any order made to telecoms and other designated operators. While secrecy might be warranted in some circumstances, it should not be the default or allowed to remain indefinitely. Such excessive secrecy shields accountability, undermines trust and precludes our members and, indeed, all Canadians from being able to understand how government uses its powers and hold it to account.

Third, Bill C-26 allows the minister to require telecoms and designated operators to disclose personal and de-identified information. Once collected, the information can be shared across "government 2.0" and with foreign entities, and easily re-identified in many cases. PACC members work hard every day to safeguard privacy. It is alarming to know that their work risks being undercut by the secret stroke of a minister's pen.

Fourth, Bill C-26 dramatically expands the Canadian Security Establishment Canada's, or CSE's, ability to obtain personal information from telecoms, financial institutions and many other companies that Canadians now trust, but it lacks the safeguards needed to constrain how the CSE can use that information. Indeed, the testimony of CSE officials makes it clear that they fully intend to use the information that they gather for both offensive and defensive purposes, and share it with their Five Eyes partners.

L'absence, dans le projet de loi C-26 d'un système de freins et contrepoids essentiel à la démocratie pour limiter ces pouvoirs dangereusement larges, a déclenché une avalanche de critiques, parce que ce n'est pas un jeu à somme nulle. Je crois que nous reconnaissons tous l'importance de la cybersécurité, mais pas au détriment de nos libertés civiles. Je tiens à souligner le travail des membres de l'autre endroit, qui ont contré les excès les plus flagrants du projet de loi, mais malgré cela, le projet de loi C-26 comprend d'importantes lacunes qui risquent de compromettre les libertés civiles et la cybersécurité. Je vais vous donner deux ou trois exemples concrets.

Premièrement, le projet de loi C-26 permet au gouvernement d'ordonner aux fournisseurs de services de télécommunications de se plier à des normes qui, en réalité, affaiblissent le chiffrement et la confidentialité. Cela met en danger la liberté de tous les Canadiens, y compris des représentants politiques, de prendre part en toute sécurité aux communications et aux échanges commerciaux nationaux et internationaux et de jouir de communications privées.

Deuxièmement, le projet de loi C-26 permet au gouvernement de garder secrète, jusqu'à nouvel ordre, toute ordonnance visant les fournisseurs de services de télécommunication et d'autres exploitants désignés. Même si la non-divulgation pouvait être justifiée dans certaines circonstances, elle ne devrait pas être l'option par défaut ni être permise jusqu'à nouvel ordre. Un secret excessif à ce point empêche la reddition de comptes, mine la confiance et empêche nos membres et, en fait, tous les Canadiens, de comprendre comment le gouvernement utilise ses pouvoirs et de lui demander des comptes.

Troisièmement, le projet de loi C-26 permet au ministre d'obliger les fournisseurs de services de télécommunication et les exploitants désignés à divulguer des informations personnelles et dépersonnalisées. Une fois recueillie, l'information pourrait être diffusée dans l'ensemble du « gouvernement 2.0 » et communiquée à des entités étrangères, et, dans de nombreux cas, elle est facilement repersonnalisable. Les membres du Conseil du Canada de l'accès et la vie privée mettent les bouchées doubles, chaque jour, pour protéger les renseignements personnels. C'est alarmant de savoir que leur travail risque d'être miné par un trait de crayon secret du ministre.

Quatrièmement, le projet de loi C-26 augmente nettement la capacité du Centre de la sécurité des télécommunications Canada d'obtenir des informations personnelles auprès d'entreprises de télécommunications, d'institutions financières et de nombreuses autres entreprises auxquelles les Canadiens font présentement confiance, mais aucune mesure de protection n'est mise en place pour limiter l'utilisation que le CST peut en faire. En effet, les témoignages des fonctionnaires du CST montre clairement qu'ils veulent utiliser l'information recueillie tant pour l'attaque que la défense, et qu'ils vont la partager avec leurs partenaires du Groupe des cinq.

In short, this legislation remains fundamentally flawed from a privacy perspective. That's why we, along with other civil society organizations and experts across Canada, have submitted recommendations to address these flaws.

Let me be clear and echo my colleagues here on the panel. We want to fix this legislation, not kill it. We recognize that cybersecurity is a team sport and that public trust is critical for this to be a win. But a bill that fails the democratic legitimacy test will fail to strengthen cybersecurity and trust. I know there has been some discussion about not letting the perfect be the enemy of the good, but in its current form, with respect, Bill C-26 is far from good. It needs fixing, and it is fixable.

If adopted, our proposed amendments, which are balanced, practical and achievable, will result in a cybersecurity framework that all Canadians can trust. Given the Senate's constitutional role, you have a critical part to play in ensuring that Bill C-26 delivers strong cybersecurity.

Senators, you have the ability to amend Bill C-26 to broaden oversight of its implementation and operation to ensure it protects privacy, delivers genuine accountability and upholds the rights of everyone in Canada. I look forward to your questions.

**The Chair:** Thank you. Ms. Polsky.

We will now we will proceed to questions. As usual, four minutes allotted to each question, including the answer. I ask that you keep your questions succinct in an effort to allow as many interventions as possible. I offer our first question to our deputy chair, Senator Dagenais.

[*Translation*]

**Senator Dagenais:** My question is for Mr. Shipley. Just last week, the government authorized its agencies to advertise on TikTok, yet it is telling us to proceed with caution if we use it. That's surprising, especially considering the warnings issued by the former director of the Canadian Security Intelligence Service, David Vigneault.

Basically, government agencies can advertise on a platform they consider hazardous to Canadian citizens. Does this indicate that the government doesn't always take cybersecurity issues affecting its citizens very seriously? I'd like your thoughts on that.

Bref, le projet de loi est fondamentalement vicié, d'un point de vue de la protection des renseignements personnels. C'est pourquoi nous, avec d'autres organisations de la société civile et experts, de tout le Canada, avons émis des recommandations afin de régler ces problèmes.

Comprenez-moi bien. Je fais l'écho de ce que mes collègues ont dit ici, pendant la séance. Nous voulons corriger le projet de loi, pas le rejeter. Nous savons que la cybersécurité est un sport d'équipe et que la confiance du public est essentielle pour que cela soit une réussite. Mais un projet de loi qui échoue au test de la légitimité démocratique ne sera pas en mesure de renforcer la cybersécurité et la confiance. Je sais que certains ont dit qu'il ne fallait pas laisser le mieux devenir l'ennemi du bien, mais, dans sa forme actuelle, le projet de loi C-26, sans vouloir vous offenser, est loin d'être bon. Il doit être corrigé et il peut l'être.

S'ils sont adoptés, les amendements que nous proposons, qui sont équilibrés, concrets et réalisables, se traduiront par un cadre de cybersécurité auquel les Canadiens peuvent avoir confiance. Compte tenu du rôle constitutionnel du Sénat, vous avez un rôle critique à jouer afin d'assurer que le projet de loi C-26 débouche sur une cybersécurité robuste.

Mesdames les sénatrices, messieurs les sénateurs, vous pouvez amender le projet de loi C-26 pour élargir la supervision de sa mise en œuvre et de son application pour vous assurer qu'il protège les renseignements personnels, établit une véritable responsabilisation et défend les droits de tous les Canadiens. J'ai hâte d'entendre vos questions.

**Le président :** Merci, madame Polsky.

Nous allons maintenant passer aux questions. Comme à l'habitude, vous aurez quatre minutes pour poser vos questions et entendre la réponse. Veuillez faire preuve de concision afin de permettre le plus grand nombre d'interventions possibles. J'offre à notre vice-président, le sénateur Dagenais, la première question.

[*Français*]

**Le sénateur Dagenais :** Ma question s'adresse à M. Shipley. Pas plus tard que la semaine dernière, le gouvernement a autorisé ses agences à faire de la publicité sur le réseau social TikTok, dont il nous demande de nous méfier comme utilisateurs. C'est pour le moins surprenant, surtout quand on se rappelle les mises en garde de l'ancien directeur du Service canadien du renseignement de sécurité, David Vigneault.

En résumé, les agences gouvernementales pourront faire de la publicité sur un réseau qu'ils considèrent comme dangereux pour les citoyens canadiens. Est-ce qu'on est devant un gouvernement qui ne prend pas toujours au sérieux les enjeux de cybersécurité pour ses citoyens? J'aimerais savoir ce que vous en pensez.

[*English*]

**Mr. Shipley:** Thank you so much for the opportunity to talk about this. I have spoken to the media about this particular issue. There is, obviously, an incongruity between what I think is a very significant national security threat — because it certainly takes a great deal of action to get a minister of the Crown to take the actions they have now proposed to take with TikTok to shutdown business operation. If we take that on the surface as true and valid — there is a body of evidence to support that TikTok's ownership structure ties back to the Chinese Communist Party and is bad for Canada — then it is foolish to spend money on advertisements there. As I pointed out to the reporter, first of all, if you're saying you can't trust this company, and you're going to give them millions of dollars in ad money to run ads, how do you know they even ran the ads? You can't trust them. It's not the first time that we have seen national security and political interests on two different tracks. I think it would be great if we could have a consistent message.

Unfortunately, with the change in government expected in the United States, the TikTok expulsion is probably not going to happen now. I think the whole issue of social media ownership, beneficial ownership and manipulation requires a serious adult conversation in this country, and we're not getting that leadership right now.

[*Translation*]

**Senator Dagenais:** You've already commented publicly on the theft of personal information in the health sector, for example. I'm talking about major pharmacy chains that have that kind of sensitive information on their computers. Are you satisfied that Bill C-26 does enough to address that? Does it reassure you in that regard? What risks are Canadian citizens exposed to in terms of their personal medical information?

[*English*]

**Mr. Shipley:** This bill does absolutely nothing to protect Canadian health care system privacy or the availability of health care in this country, purposely so because it was determined to limit to the federal scope.

My ardent support of getting this done is born out of hope that we can move on to much-needed other conversations. When we talk about this, in Newfoundland, an interviewer — and I encourage you to go back and see the CBC coverage of this — as the crisis unfolded, he asked if the information included people's reason for being admitted to a hospital in Newfoundland, to which the answer was "yes." That meant every person who went for an abortion in that province had that information potentially exposed.

[*Traduction*]

**M. Shipley :** Merci de me donner l'occasion d'en parler. J'ai parlé aux médias de cet enjeu en particulier. Il y a, évidemment, une incohérence entre ce que je crois être une importante menace de sécurité nationale... Parce que, il faut déployer beaucoup d'efforts pour convaincre un ministre de la Couronne de mettre en œuvre les mesures proposées pour TikTok, soit de mettre fin aux activités de l'entreprise. Si nous jugeons que cela est vrai et valide — et les preuves montrent que les propriétaires de TikTok sont liés au Parti communiste de la Chine et que l'application est mauvaise pour le Canada —, eh bien, il est absurde de dépenser de l'argent pour faire de la publicité sur la plateforme. Comme je l'ai dit au journaliste, premièrement, si vous dites que vous ne pouvez pas faire confiance à l'entreprise, et que vous leur donnez ensuite des millions de dollars en recettes publicitaires pour qu'elle diffuse vos publicités, comment pouvez-vous savoir qu'elle a bel et bien diffusé les publicités? Vous ne pouvez pas lui faire confiance. Ce n'est pas la première fois que la sécurité nationale et les intérêts politiques sont sur des voies divergentes. J'aimerais bien qu'il y ait un message cohérent.

Malheureusement, en raison des changements de gouvernement attendus aux États-Unis, l'interdiction de TikTok n'aura probablement pas lieu. Je crois que le Canada doit tenir des discussions sérieuses sur les questions de la propriété des réseaux sociaux, de la propriété effective et de la manipulation, et nous ne voyons pas présentement ce genre d'initiative.

[*Français*]

**Le sénateur Dagenais :** Vous avez déjà fait publiquement des commentaires sur les vols de données personnelles dans le domaine de la santé, entre autres. Je parle ici des ordinateurs de grandes chaînes de pharmacies qui ont ce genre d'informations sensibles. J'aimerais savoir si le projet de loi C-26 vous satisfait et vous rassure à ce sujet. Quels sont les risques que courent les citoyens canadiens en ce qui a trait à leurs données médicales personnelles?

[*Traduction*]

**M. Shipley :** Rien dans le projet de loi ne protège la confidentialité du système de santé ou l'accessibilité des soins de santé, au Canada, en particulier parce que l'on a voulu limiter la portée des compétences fédérales.

Si je soutiens cela avec autant d'ardeur, c'est parce que j'espère que nous pourrons passer à d'autres discussions très importantes. Lorsque nous avons parlé de cela, à Terre-Neuve, un journaliste — et je vous encourage à consulter la couverture de CBC/Radio-Canada sur le sujet —, quand la crise s'est déclarée, a demandé si l'information comprenait les motifs d'admission à l'hôpital de Terre-Neuve, et la réponse a été : « oui ». Cela signifie que l'information de toutes les femmes de la province qui avaient subi un avortement pourrait avoir été divulguée.

Not just that, we think about privacy and we think of the horrible implications. Years ago, we had a LifeLabs breach that involved people's sensitive blood tests. We also have five hospitals in Ontario that were crippled for a period of time. What we know from U.S. studies and the World Health Organization is that when hospitals go down, patient outcomes suffer. People die. I could not put it more plainly.

The inability of this country to get beyond a Constitution that was thought of in the 19th and 20th centuries to contend with 21st century problems is a big issue. I don't care that health care is a province's jurisdiction. If I can tie outcomes to hip surgery, I can tie cybersecurity to federal government funding. I don't understand what it takes to get the government to care.

**Senator Kutcher:** Thank you very much for being here. I just want to follow up on Senator Dagenais's issues around the health care issue. Any of you may please comment on this.

The reality is that health care is primarily a provincial and territorial responsibility, and it is fiercely guarded as such. The federal government does have primary authority for some parts of health care, such as the military, the RCMP and Indigenous populations.

Cybersecurity issues around health care — my way of thinking, and I could be wrong on this — cluster into two areas, one being personal health data — the privacy side — and the other being the health care infrastructure — the ability to run your hospital, make sure that the electricity doesn't shut off the intensive care unit, or ICU, beds, et cetera.

Given those multiple challenges and given that this legislation is federal, do you have suggestions or thoughts as to how we can deal with this health care conundrum through this piece of legislation?

**Ms. Polsky:** I would love to offer a few comments.

One of the things that I have seen is that, yes, security is important, but we don't have enough people who know what they are doing or are properly trained to actually make sure that systems are secure. There are vulnerabilities. Every system, even a key-lock system, has workarounds because whatever the technology is, the biometric is to let you into the office and I don't happen to have that, whether it's a fingerprint, an eye scan or whatever, there has to be a workaround. Otherwise, you might be considered to be discriminating against me for health reasons. So there is always a flaw.

Nous pensons également à la confidentialité et aux répercussions désastreuses. Il y a plusieurs années, des données sensibles sur les prises de sang ont été divulguées en raison d'une fuite à LifeLabs. Également, en Ontario, cinq hôpitaux ont été paralysés pendant un certain temps. Selon des études américaines et l'Organisation mondiale de la santé, lorsque les hôpitaux arrêtent de fonctionner, cela a des répercussions sur les patients. Des patients meurent. Je ne peux pas le dire plus explicitement.

L'incapacité du Canada à aller au-delà de la Constitution, qui a été pensée aux XIX$^{e}$ et XX$^{e}$ siècles, pour régler les problèmes du XXI$^{e}$ siècle, est un enjeu important. C'est sans importance pour moi que le système de soins de santé relève de la compétence provinciale. Si je peux lier des résultats à une chirurgie de la hanche, je peux lier la cybersécurité au financement du gouvernement fédéral. Je ne sais pas ce qu'il faut faire pour que le gouvernement s'en soucie.

**Le sénateur Kutcher :** Merci beaucoup d'être venus ici. Je veux simplement enchaîner sur ce que le sénateur Dagenais a dit à propos des soins de santé. Vous êtes tous invités à commenter la question.

Dans les faits, les soins de santé relèvent principalement de la compétence provinciale et territoriale, et cela est férocement défendu. Le gouvernement fédéral a le dernier mot pour certains aspects de la santé, ceux qui concernent par exemple l'armée, la GRC et les populations autochtones.

Les questions de la cybersécurité en santé — c'est ce que je pense, et je peux me tromper — se classent dans deux groupes. Il y a d'une part les données médicales personnelles — les renseignements personnels — et de l'autre, l'infrastructure de la santé — la capacité à faire fonctionner l'hôpital, à s'assurer que l'électricité n'est pas coupée dans les unités de soins intensifs, dans les chambres, et cetera.

Compte tenu de ces nombreux défis et du fait qu'il s'agit d'un projet de loi fédéral, avez-vous des suggestions ou des commentaires sur la façon dont ce projet de loi permettrait de résoudre ce dilemme des soins de santé?

**Mme Polsky :** J'aimerais beaucoup m'exprimer sur le sujet.

L'une des choses que j'ai vues est que, oui, la sécurité est importante, mais il n'y a pas assez de gens qui savent ce qu'ils font ou qui sont suffisamment formés pour assurer réellement la sécurité des systèmes. Il y a des vulnérabilités. Tous les systèmes, même un système de verrouillage à clé, peuvent être contournés, parce que, peu importe la technologie, le but des systèmes biométriques est de vous donner accès au bureau, et si je n'ai pas ça, une empreinte digitale, un balayage oculaire, peu importe, il doit y avoir un moyen de le contourner. Autrement, on pourrait dire que vous faites de la discrimination fondée sur l'état de santé. Donc, il y a toujours une faille.

That's one side of it. That's the operational side.

From a privacy side, when anybody goes onto a website — and this is regarding a vast majority of websites, including the Canadian Association for Mental Health. I did a quick scan of their website over a year ago, then a few months later and a few months later. Never mind the massive amount of cookies — like 58 of this type and 35 of that type — which are sending information to other websites. Before you even see the website, the fact that you are there requesting that website has been communicated secretly to Meta, which is Facebook. You fill in a form that says, "I want to contact you." Why would I want to contact you? Incest, suicide, mental health — whatever — that information has been communicated.

If somebody gets a hold of that, it's not just whether I went to a hospital and why; this is a completely different matter. This is around mental health issues. That makes somebody vulnerable if there is an interested party who wants to use that information.

That is a huge risk. Yes, it's health information, but it's federal because it falls under the Personal Information Protection and Electronic Documents Act, or PIPEDA, and — forgive me for straying — Bill C-27 won't improve that situation.

**Mr. Warnell:** I'll offer a perspective to your question, senator.

We define 10 critical infrastructure sectors in Canada. This bill expressly talks to four that the federal government has more direct control over. It is an important first step in driving the conversation around the requirements and the capabilities to ensure safe outcomes in those sectors, and it can set a trailblazing path toward informing and working through collaboration with the various levels of government, whether provincial or municipal, on the importance of this topic.

We could, as individual Canadians and in this body, talk about how we can make the bill more inclusive and cast its net wider, but at the same time, the threat landscape continues to evolve. Standing still in defence of "hey, we should go further into health or further into food or water systems," I think, would be a disservice to the threat that is happening right now. The first step will be the most important step, and then we can continue to tackle and model what "good" looks like across other critical infrastructure sectors as well.

C'est l'un des aspects. C'est l'aspect opérationnel.

Du point de vue de la protection des renseignements personnels, lorsqu'une personne visite un site Internet — et cela s'applique à la grande majorité des sites Internet, y compris celui de l'Association canadienne pour la santé mentale. J'ai consulté rapidement son site Internet, il y a plus d'un an, puis, quelques mois plus tard, et deux ou trois autres mois plus tard. L'important, ce n'est pas le nombre incroyable de témoins, par exemple 58 cookies de ce type et 35 cookies de cet autre type, qui transmettent l'information à d'autres sites Web. Avant même que s'ouvre le site Web, le fait que vous l'avez recherché a été secrètement communiqué à Meta, qui est Facebook. Vous envoyez un formulaire qui dit : « Je veux communiquer avec vous. » Pourquoi voudrais-je communiquer avec eux? Inceste, suicide, santé mentale, peu importe, l'information a été transmise.

Si l'information tombe entre les mains de quelqu'un, il ne s'agit pas simplement d'informations concernant ma visite à l'hôpital et le motif de ma visite; c'est une question tout autre. Il est question de santé mentale. La personne est à risque si une partie intéressée souhaite utiliser l'information.

C'est un énorme risque. Oui, ce sont des données médicales, mais elles relèvent de la compétence fédérale, conformément à la Loi sur la protection des renseignements personnels et les documents électroniques, et — je m'excuse d'avoir dévié du sujet — le projet de loi C-27 n'améliorera aucunement la situation.

**M. Warnell :** Sénateur Kutcher, je vais donner mon point de vue sur votre question.

Nous avons défini 10 secteurs d'infrastructure critiques, au Canada. Le projet de loi parle explicitement des quatre secteurs sur lesquels le gouvernement fédéral a un contrôle plus direct. C'est une première étape importante si l'on veut discuter des exigences et des capacités et assurer des résultats sécuritaires dans ces secteurs. Cela pourrait être une nouvelle façon d'informer les différents ordres du gouvernement et de collaborer avec eux, que ce soit les gouvernements provinciaux ou les administrations municipales, dans cet important dossier.

Nous pourrions, en tant que Canadiens et membres d'un organisme, discuter de la manière de rendre le projet de loi plus inclusif et de lui donner plus de portée, mais, en même temps, l'environnement de la menace est en constante évolution. Je crois que ne rien faire et dire : « hé, nous devrions traiter plus en détail des systèmes de la santé, de l'alimentation et de l'eau », serait désavantageux, étant donné la menace actuelle. La première étape sera la plus importante, et puis, nous pourrons continuer de définir et de modéliser ce qu'est une « bonne chose » également dans l'ensemble des secteurs de l'infrastructure critique.

**Mr. Shipley:** There are things the government could do very quickly. They could actually form a centre of excellence in what ideal state health care cybersecurity at a provincial level should look like. They could get agreements with each of the provinces — because no province says no to more money — to say that, in exchange for this net new funding, here are the digital security standards we could get to. Health Canada could play a better role in making sure that medical devices are actually secure by design and updated. They could coordinate better with the provinces on that.

We could be forming better agreements with the provinces to respond and share lessons learned through a cybersecurity review board that, when a hospital gets hit, asks how it happened. We should be as transparent with a hospital ransomware incident as we are with a plane crash, because it causes harm and we need to learn everything we can from it.

Those are all things they could do now.

**Senator M. Deacon:** Thank you for being here today.

I would like to address my first question to Mr. Warnell, if you don't mind. It concerns international cooperation.

Last year, the Bruce Power site took part in a blended cyber and physical mock attack with industry peers at the Los Alamos National Laboratory in New Mexico, something I understand that was a first-of-its-kind simulation. I am wondering how important peer-to-peer cooperation is for you. Is it easy enough to share this kind of information with trusted international peers in your industry? Also, does this bill in any way assist, enhance or hinder security cooperation?

**Mr. Warnell:** Thank you for your question.

The exercise we did complete through the Canadian national labs in conjunction with national labs down in the United States was, in fact, the first blended joint cyber-physical full-scale security exercise in the nuclear industry. It demonstrated a number of key elements. Cross-border allyship is important to driving lessons learned and expanding our body of knowledge around where we can enhance our defences and capabilities from a different point of view from what we had solely in the Canadian nuclear landscape.

We benefit within the nuclear industry of having both national and international networks of operational experience sharing what we have benefitted from, for decades. We draw upon that, whether it's about getting better at work-management practice in

**M. Shipley :** Le gouvernement peut prendre des mesures rapidement. Il pourrait créer un centre d'excellence pour déterminer l'idéal en matière de cybersécurité des soins de santé, à l'échelon provincial. Il pourrait conclure une entente avec chaque province — parce qu'aucune province ne refuserait de l'argent supplémentaire — pour dire que, en échange du nouveau financement, voilà les normes en matière de sécurité numérique que vous devez respecter. Santé Canada pourrait jouer un plus grand rôle afin d'assurer que les appareils médicaux sont conçus de manière sécuritaire et mis à jour. Le ministère pourrait collaborer davantage avec les provinces à ce chapitre.

Nous pourrions conclure de meilleures ententes avec les provinces et faire circuler les leçons apprises par l'entremise d'un comité d'examen de la cybersécurité qui, lorsqu'un hôpital est attaqué, se demanderait comment cela a pu être possible. Nous devrions faire preuve de transparence pour les incidents de rançongiciel des hôpitaux, comme nous le faisons pour les accidents d'avion, parce que c'est ce qui cause des préjudices et que nous devons en tirer le plus de leçons possible.

Ce sont toutes des choses qui pourraient être faites maintenant.

**La sénatrice M. Deacon :** Merci d'être présents aujourd'hui.

J'aimerais poser ma première question à M. Warnell, si vous le permettez. Elle concerne la coopération internationale.

L'année dernière, les installations de Bruce Power ont participé à une simulation d'attaque mixte informatique et physique avec des pairs du laboratoire national de Los Alamos, au Nouveau-Mexique; si j'ai bien compris, il s'agissait de la première simulation de ce genre. Quelle importante accordez-vous à la coopération entre pairs? Est-ce facile de communiquer ce genre d'information avec des pairs auxquels vous faites confiance à l'international, au sein de votre industrie? Aussi, est-ce que ce projet de loi va d'une façon ou d'une autre améliorer ou freiner la coopération en matière de sécurité?

**M. Warnell :** Merci de la question.

L'exercice que nous avons effectivement fait dans les laboratoires nationaux canadiens en collaboration avec les laboratoires nationaux aux États-Unis était, oui, le premier exercice de sécurité mixte complet jumelant une attaque informatique et physique dans le secteur de l'énergie nucléaire. Il a montré un certain nombre d'éléments clés. Il est important d'avoir des alliés de l'autre côté de la frontière pour profiter des leçons retenues et améliorer nos connaissances sur la façon dont nous pouvons améliorer nos défenses et nos capacités en fonction d'un autre point de vue que le seul que nous avons du paysage nucléaire canadien.

Dans l'industrie nucléaire, nous avons la chance d'avoir des réseaux tant nationaux qu'internationaux où nous partageons nos expériences opérationnelles, et nous en bénéficions depuis des décennies. Nous nous appuyons sur ces réseaux, que ce soit pour

the factory or power plant, or in a better supply chain practice or cybersecurity practice. That ability to share across borders and with trusted international partners is paramount to securing capabilities and driving maturity of what we do every single day. We've had that in place for many decades.

This particular legislation, as it becomes part of Canada's landscape, sends a signal to our international partners that we are taking cybersecurity seriously, and it welcomes us to the table of those important conversations where those practices and learnings about the threat landscape — that could be changing or emerging — gets shared. It could be a preventative approach for the Canadian landscape versus being left on the outside.

I think it very much is an important element of international cooperation to ensure that we can be best informed to either prevent and/or respond to events as they unfold.

**Senator M. Deacon:** Thank you.

Mr. Shipley, in the past, you've appropriately expressed some concerns around the regulatory making process that will follow this bill, stating to the Canadian Chamber of Commerce earlier this year that the regulations, such as the Office of the Superintendent of Financial Institutions, or OFSI, are experienced, but others are being given this responsibility for cyber for the first time.

The minister, when he appeared, said there will be a very thorough consultation process in crafting the regulations. I'm wondering if that statement eases some of your concerns, heightens some of your concerns or what you might suggest to the government to lead them in the right direction?

**Mr. Shipley:** I am open to the regulatory review process and what that could unfold. I think my concern is going to be more about how things get executed at the departmental level, and I don't think regulations are going to do that. It's going to come down to who they have and the talent, the resourcing and experience that they'll have.

Telecommunications is really important to us, and they previously had a very collaborative relationship through the Canadian Security Telecommunications Advisory Committee, or CSTAC, so industry and government working side by side. Now, you are going to have a regulator responsibility, and if we have people that don't have the experience on the government side making a regulatory call, they could potentially cause more harm

établir de meilleures pratiques de gestion du travail dans les usines ou les centrales électriques ou de meilleures pratiques liées à la chaîne d'approvisionnement ou à la cybersécurité. Cette capacité de communiquer de l'information de l'autre côté des frontières à des partenaires internationaux auxquels nous faisons confiance est essentielle pour renforcer nos capacités et devenir meilleurs dans ce que nous faisons chaque jour. Nous le faisons depuis de nombreuses décennies.

Ce projet de loi, qui fera partie du paysage du Canada, envoie un signal à nos partenaires internationaux et les informe que nous prenons la question de la cybersécurité au sérieux; nous serons alors accueillis aux tables où se tiennent ces conversations importantes sur les pratiques et les apprentissages au sujet du paysage des menaces, lesquelles pourraient changer ou se renouveler. Il pourrait s'agir d'une approche préventive pour le paysage canadien, qui pourrait autrement être laissé de côté.

Il faut nous assurer d'être le mieux informés possible pour prévenir les incidents ou y réagir quand ils surviennent. Je pense que c'est vraiment un élément important de la coopération internationale.

**La sénatrice M. Deacon :** Merci.

Monsieur Shipley, par le passé, vous avez à juste titre exprimé des préoccupations au sujet du processus de réglementation qui suivra ce projet de loi, et vous avez déclaré, plus tôt cette année, devant la Chambre de commerce du Canada que les organismes de réglementation, comme le Bureau du surintendant des institutions financières, le BSIF, ont de l'expérience, mais que d'autres sont chargés de la cybersécurité pour la première fois.

Le ministre, quand il a comparu, a dit qu'il y aurait un processus de consultation complet pendant l'élaboration de la réglementation. Est-ce que cette déclaration dissipe quelque peu vos préoccupations et en aggrave-t-elle d'autres? Que suggéreriez-vous au gouvernement pour qu'il prenne la bonne direction?

**M. Shipley :** Je suis ouvert à l'idée d'un examen réglementaire et à ce que celui-ci pourrait révéler. Je crois que je m'inquiète davantage de la façon dont les choses sont faites au sein des ministères et je ne pense pas que les règlements vont remplacer cela. Tout reposera en fin de compte sur le personnel de ces organisations, leurs talents, leurs ressources et leur expérience.

Les télécommunications sont très importantes pour nous, et par le passé, le secteur collaborait beaucoup grâce au Comité consultatif canadien pour la sécurité des télécommunications, le CCCST, de sorte que l'industrie et le gouvernement travaillaient côte à côte. Maintenant, il y aura un responsable sur le plan de la réglementation, et, si on a des gens au gouvernement qui n'ont pas d'expérience et qui prennent des décisions en matière de

than good if they don't have the experience. It's going to take years for them to build that up.

We are expecting Innovation, Science and Economic Development Canada, or ISED, to arrive at the same specification that OSFI has had 30 years to build to. It's in the execution of this that we will succeed or fail.

**Senator Cardozo:** My question is for Mr. Warnell.

I wonder if you could just tell us a little bit more about the cybersecurity threat that you face, without going into too much detail — this is a public meeting — and how you cooperate with the other partners across the country who are either producing or dealing with nuclear power in one way or another?

**Mr. Warnell:** Absolutely. Thank you for your question.

Given that this is a public forum, I'll keep it to what has been publicly disclosed. What has been disclosed in the threat landscapes facing critical infrastructure in North America over the last two years have been unprecedented. The volume of unclassified information — you might have heard of threat actors known as Volt Typhoon and Salt Typhoon, for example. You will hear large disclosures through our joint partners in the Five Eyes around the threat these Chinese national state actors and aligned actors are prepositioning in critical infrastructure, including the electrical distribution network, in the event of a larger scale geopolitical challenge.

This would have been previously — I would say — very tightly held pieces of information. The threat is so imminent and so real that our intelligence communities have been able to work through the various channels to get that information declassified, to talk about the importance of it to the public and to us in areas of particular influence or power to make differences and to drive change. That's to speak to the threat landscape.

Through that, we work — much like other critical infrastructure industries — with our industry peers to share operating experience or operating intelligence across our organizations to see if a particular threat of someone knocking at our door is impacting other infrastructure operators. As well, through the Energy Security Technical Advisory Committee, or E-STAC — which is the equivalent to CSTAC — has formed, coming out of the events last year at Suncor, where they suffered a major ransomware event and really pushed the energy providers outside of nuclear to come together and start to operate as one party in defence of our operations.

réglementation, cela pourrait faire plus de mal que de bien, s'ils n'ont pas l'expérience. Cela va leur prendre des années, acquérir cette expérience.

On s'attend à ce qu'Innovation, Sciences et Développement économique Canada, ou ISDE, arrive au même résultat que le BSIF, qui a eu 30 ans pour arriver à ce résultat. C'est l'exécution qui sera une réussite ou un échec.

**Le sénateur Cardozo :** Ma question s'adresse à M. Warnell.

Pourriez-vous nous en dire un peu plus sur la menace de cybersécurité à laquelle vous faites face, sans aller trop dans les détails — il s'agit d'une réunion publique — et sur la façon dont vous coopérez avec les autres partenaires dans tout le pays qui produisent de l'énergie nucléaire ou qui utilisent de l'énergie nucléaire d'une façon ou d'une autre?

**M. Warnell :** Absolument. Merci de la question.

Comme il s'agit d'une tribune publique, je vais m'en tenir à ce qui a été divulgué publiquement. Ce qui a été divulgué en ce qui concerne les paysages de menace pour les infrastructures essentielles en Amérique du Nord ces deux dernières années est sans précédent. Le volume d'informations non classifiées... Vous avez peut-être entendu parler des auteurs de menaces connus sous le nom de Volt Typhoon et Salt Typhoon, par exemple. Vous allez entendre de nos partenaires du Groupe des cinq beaucoup d'informations au sujet de la menace que représentent ces acteurs nationaux chinois relevant de l'État et d'États associés qui se préparent à attaquer des infrastructures essentielles, y compris le réseau de distribution électrique, si jamais il y a un enjeu géopolitique de grande envergure.

Je dirais que cette information aurait jadis été gardée très secrète. La menace est si imminente et si réelle que nos organismes de renseignement ont pu déclassifier cette information, par divers moyens, pour pouvoir nous la donner, au public et à nous, qui œuvrons dans des sphères d'influence et de pouvoir précis et qui pouvons faire une différence et favoriser le changement. Voilà ce que j'avais à dire du paysage de la menace.

À cet égard, nous travaillons — comme beaucoup d'autres industries liées aux infrastructures essentielles — avec nos pairs de l'industrie pour échanger notre expérience opérationnelle et nos renseignements opérationnels avec toutes les organisations pour savoir si une menace précise, si quelqu'un qui frappe à la porte, a une incidence sur d'autres exploitants des infrastructures. Aussi, quand le *Energy Security Technical Advisory Committee*, ou l'E-STAC, qui est l'équivalent du CCCST, s'est formé, à la suite des événements survenus l'année dernière à Suncor, victime d'un incident majeur impliquant un rançongiciel, ce qui a vraiment forcé les autres fournisseurs d'énergie autres que d'énergie nucléaire à se relever les manches tous ensemble et à commencer à agir comme une seule entité pour défendre nos activités.

It's been a really good change, over the last 18 months to 2 years. The threat is real. It has been publicly disclosed, and, again, it is why standing still is not an option for Canada or for any other allied nation.

**Senator Cardozo:** Thanks. If I have a little bit of time, just make this a quick response by Mr. Shipley and Ms. Polsky.

In terms of other sectors, is it possible that we get to this down the road when we deal with the sectors we're covering here? Ms. Polsky, I think you're saying that's not the issue. There are just some issues around civil liberties that need to be fixed that cannot be fixed later.

**Ms. Polsky:** Issues around civil liberties need to be addressed now, but I also look at the practical side of implementing this legislation. Really, every organization in Canada, whether it's federally regulated or not — health care — they all, long ago, were supposed to be doing all of the things that we're talking about today: Securing their networks, training their people and having policies in place so they can comply with the privacy laws.

This is going to be another massive onus and huge obligation on organizations of all sorts. They're already behind the eight ball.

**Mr. Shipley:** We need to get this done, because we can't keep the lights on and the natural gas flowing. That's a primal survival issue for us. We have to get moving, as Mr. Warnell said. Again, we almost had a pipeline explode in this country, so we must move. We can't stop here, and if we wait another 10 years, there is so much Canadian suffering we are not going to prevent.

With respect to the privacy laws — which my colleague is more suited to — I'll say this: Our laws are toothless. There are no consequences in this country. The reason people don't spend money is because when organizations realize there is no consequence, they go to other risks.

Privacy and security are linked. If there are no consequences, they don't invest in privacy, and when they don't invest in privacy, they aren't secure either.

Cela a été un changement très positif, au cours des 18 derniers mois, voire des deux ans qui ont passé depuis. La menace est réelle. Cette information a été divulguée publiquement, et encore une fois, c'est pour cette raison que le Canada ou n'importe quel autre des pays alliés n'ont pas l'option de ne rien faire.

**Le sénateur Cardozo :** Merci. S'il me reste encore un peu de temps, j'aimerais que M. Shipley et Mme Polsky répondent rapidement à ma question.

En ce qui concerne les autres secteurs, est-il possible de mettre cela en œuvre, plus tard, dans les autres secteurs dont il est question ici? Madame Polsky, je pense que vous dites que ce n'est pas le problème. Il y a seulement des problèmes concernant les libertés civiles qui doivent être réglés maintenant, et pas plus tard.

**Mme Polsky :** Les problèmes qui touchent les libertés civiles doivent être réglés maintenant, mais je pense aussi à l'aspect pratique de la mise en œuvre de ce projet de loi. Vraiment, chaque organisation au Canada, qu'elle relève du fédéral ou pas — la santé — était depuis longtemps censée faire toutes les choses dont nous parlons aujourd'hui : sécuriser ses réseaux, former son personnel et mettre en œuvre des politiques afin de respecter les lois sur la protection des renseignements personnels.

Ce sera un autre fardeau énorme et une grande obligation pour toutes les organisations. Elles sont déjà en retard.

**M. Shipley :** Il faut que cela se fasse, parce que nous ne pouvons pas laisser l'éclairage allumé et le gaz naturel couler. C'est un enjeu de survie primordial pour nous. Nous devons vraiment faire quelque chose, comme l'a dit M. Warnell. Encore une fois, un oléoduc a failli exploser, dans notre pays, donc nous devons agir. Nous ne pouvons pas nous arrêter ici, et si nous attendons encore 10 ans, nous ne pourrons pas empêcher que les Canadiens souffrent.

En ce qui concerne les lois sur les renseignements personnels — un sujet que mon collègue connaît mieux —, voici ce que je dirais : nos lois n'ont pas de mordant. Il n'y a pas de conséquence dans notre pays. Les gens ne dépensent pas d'argent parce que, quand les organisations réalisent qu'il n'y a pas de conséquence, elles passent à d'autres risques.

La protection des renseignements personnels et la sécurité sont liées. S'il n'y a pas de conséquences, on n'investit pas dans la protection des renseignements personnels, et lorsque l'on n'investit pas dans la protection des renseignements personnels, ceux-ci ne sont pas non plus en sécurité.

[*Translation*]

**Senator Carignan:** My question is about how confident the government can be that it is in control of elements of cybersecurity. I'm talking about how the government handles attacks and its cybersecurity vulnerabilities.

When cybersecurity drills were done, also known as cybernetic simulations, only 25% of the departments did those simulations.

Is there a chance companies will lose confidence in the government, which isn't even up to standard itself? Will people and businesses have so little confidence in the government that it will be difficult to enforce Bill C-26?

[*English*]

**Mr. Shipley:** I want to be very clear that I have a lot of faith in the civil servants in this country, the hard-working men and women in various departments that are doing everything they can to protect the Government of Canada. I have had the privilege of meeting a great deal of them, and we have some tremendous talent.

What we lack in this country is a political interest in this issue, and you can see that in that they have a strategy that they just can't be bothered to decide how much they want to spend and release.

You can see that when Joe Biden got upset at what happened with the Colonial Pipeline in the United States and said, "We will respond to this threat with the whole of government," which is the same as they respond to terrorism, and we've never had our Prime Minister hold a summit in this country about the crisis. Newfoundland, Ontario, London Drugs — on and on and on — and British Columbia fully compromised by a foreign nation state to the extent of years worth of damage, and we can't get a meeting at the senior political level.

It is to the government's credit that Jennifer O'Connell is now a parliamentary secretary, which is progress. She's phenomenal, but we need prime ministerial attention because it matters when a prime minister gets up and says, "We're not going to be your punching bag or ATM anymore for cybercrime; we're getting serious." Australia has done exactly that, and they're not that different from us. We're not getting out of bed, and in the world we're walking into in 2025, that means it's open season on the maple leaf, and it's not going to be good for us.

[*Français*]

**Le sénateur Carignan :** Ma question porte sur la confiance du gouvernement en vue de s'assurer d'avoir un bon contrôle des éléments de cybersécurité. J'en viens à la manière dont le gouvernement se comporte lui-même par rapport aux attaques ou à ses vulnérabilités en matière de cybersécurité.

Lorsqu'ils ont fait les exercices de cyberpratique, qu'on appelle de la simulation cybernétique, seulement 25 % des ministères ont fait ces exercices de simulation.

Est-ce qu'il n'y a pas un risque de manque de confiance de la part des entreprises par rapport au gouvernement, qui est lui-même déficient? Les gens et les entreprises auront-ils si peu confiance dans le gouvernement que ce sera difficile d'assurer l'application du projet de loi C-26?

[*Traduction*]

**M. Shipley :** J'aimerais dire clairement que je fais tout à fait confiance aux fonctionnaires de notre pays, aux hommes et aux femmes qui travaillent dur dans divers ministères et qui font tout ce qu'ils peuvent pour protéger le gouvernement du Canada. J'ai eu le privilège d'en rencontrer un bon nombre, et nous avons énormément de talents.

Ce qui nous manque, au Canada, c'est un intérêt politique pour cet enjeu, et vous pouvez le voir dans la stratégie qu'ils ont élaborée, mais sans vouloir décider combien ils veulent dépenser ou divulguer.

On peut le voir quand Joe Biden s'est fâché à cause de ce qui est arrivé au Colonial Pipeline aux États-Unis et qu'il a dit « nous allons réagir à cette menace avec tout le poids du gouvernement », qui est la réponse qu'il donne lorsqu'il est question de terrorisme, et notre premier ministre n'a jamais tenu de sommet dans notre pays au sujet de la crise. Terre-Neuve, l'Ontario, London Drugs, et ainsi de suite, et la Colombie-Britannique, ont tous été victimes d'une attaque lancée par un pays étranger et ont subi des dommages qu'il faudra de nombreuses années pour effacer, et les plus hauts fonctionnaires sont incapables de se réunir.

C'est grâce au gouvernement que Jennifer O'Connell occupe maintenant le poste de secrétaire parlementaire, et c'est un pas dans la bonne direction. Elle est extraordinaire, mais nous devons avoir l'attention du premier ministre, parce que c'est important quand un premier ministre se lève et dit « nous n'allons pas être le souffre-douleur ni le guichet automatique des cybercriminels; nous prenons ça au sérieux maintenant ». C'est exactement ce qu'a fait l'Australie, et ce pays n'est pas différent du nôtre. Nous ne nous réveillons pas assez vite, et bientôt en 2025, cela veut dire que la guerre contre l'unifolié est ouverte, et ce ne sera pas bon pour nous.

**Ms. Polsky:** That's putting it gently, but I also look at the other side. When there is a breach — never mind an exercise to earn the public's trust — the Office of the Privacy Commissioner of Canada is notified, and that's as far as it goes. The public has no way of knowing that there has been a breach. There is one place in the world that I have found where a breach notification is publicized: California. Other than that, nowhere.

We're always told to make sure where your information is going. The onus is put on us individually, not the tech companies, not governments. How can you or I make that determination when it's opaque? As Mr. Shipley said, it's a matter of political will, which has not been evident for a very long time. We have fallen behind, and we're scrambling to catch up. That's never a good position to be in because reactive is in panic mode instead of being thoughtful, proportionate, reasonable and practical.

**Senator Richards:** You just answered my question, Ms. Polsky. In a way, this is an existential threat, and this bill is only — as has been said — a first step. Security measures might become more extreme and revamped as time passes. As a matter of fact, they're going to have to be. How can we ever keep up with the ongoing threat? If we do that, how do we better coordinate privacy and national security?

**Ms. Polsky:** Having the obligation and the liability on the executive is a tremendous idea. Think back to Enron, if anyone remembers that. Again, as Mr. Shipley said, our laws are toothless. Jennifer Stoddart said as she was leaving office that the privacy law could use more teeth. There is no penalty. Organizations can now do as they wish. That's the private sector and also the public sector, because if there is a fine it comes out of this taxpayer pocket of dollars and goes into that taxpayer pot. It's all taxpayer dollars being shuffled like a shell game, but nothing has been changing — to our detriment individually and collectively.

**Senator Richards:** Mr. Shipley, can you say that this bill is good enough or that it will be revamped within a couple of years, and will we be able to keep up with the ongoing threat?

**Mr. Shipley:** This law started in 2022, and we're still not even through the Royal Assent phase so that we can get to the regulatory work to have it implemented to even know when the phase-in date will be. As much as I wish that there were still changes to be made, I would sacrifice those changes at this point to at least get the ball moving farther and hopefully advance the

**Mme Polsky :** Ce n'est pas peu dire, mais je regarde aussi l'envers de la médaille. Lorsqu'il y a une faille — ne parlons même pas d'un exercice pour gagner la confiance du public —, on avise le Commissariat à la protection de la vie privée du Canada et c'est tout. Le public n'a aucune façon de savoir qu'il y a eu une faille. Il n'y a qu'un endroit dans le monde où j'ai vu que l'on avisait les gens qu'il y avait eu une faille : la Californie. Sinon, il n'y en a pas.

On nous dit toujours de faire attention aux endroits où on laisse nos renseignements. Le fardeau nous est imposé à nous, individuellement, et non pas aux entreprises technologiques ni aux gouvernements. Comment vous et moi pouvons-nous prendre cette décision quand c'est opaque? Comme l'a dit M. Shipley, c'est une question de volonté politique, laquelle n'est pas claire depuis très longtemps. Nous sommes à la traîne, et nous peinons à rattraper notre retard. Ce n'est jamais bien d'être dans cette position parce que nous réagissons dans la panique plutôt que de réfléchir, de soupeser, d'être raisonnables et d'être pratiques.

**Le sénateur Richards :** Vous venez de répondre à ma question, madame Polsky. D'une certaine façon, c'est une menace existentielle, et ce projet de loi, comme il a été dit, n'est qu'une première étape. Les mesures de sécurité pourraient devenir plus strictes et être mises à jour au fur et à mesure. En fait, elles devront l'être. Comment allons-nous pouvoir rester au fait des menaces continues? Si nous faisons cela, comment pouvons-nous mieux coordonner la protection des renseignements personnels et la sécurité nationale?

**Mme Polsky :** Ce serait une bonne idée d'imposer cette obligation aux hauts dirigeants et de leur demander de rendre des comptes. Rappelez-vous Enron, si quelqu'un s'en rappelle. Encore une fois, comme M. Shipley l'a dit, nos lois n'ont pas de mordant. Quand elle a quitté son poste, Mme Jennifer Stoddart a dit que la Loi sur la protection des renseignements personnels pourrait être plus sévère. Il n'y a pas de conséquence. Les organisations peuvent maintenant faire ce qu'elles veulent. C'est comme ça pour le secteur privé et le secteur public parce que, s'il y a une amende, le contribuable la paie de sa poche et l'argent retourne dans les poches du même contribuable. On fait un tour de passe-passe avec l'argent des contribuables, mais rien ne change — à notre détriment, tant personnel que collectif.

**Le sénateur Richards :** Monsieur Shipley, pouvez-vous dire que ce projet de loi est suffisant, qu'il sera remanié d'ici quelques années ou serons-nous en mesure de faire face à la menace actuelle?

**M. Shipley :** Cette loi est sur la table depuis 2022, et nous n'avons même pas obtenu la sanction royale qui nous permettrait d'entamer le travail réglementaire nécessaire à sa mise en œuvre, et nous ne savons même pas quand la date d'entrée en vigueur sera fixée. Même si j'aimerais qu'il y ait encore des changements à apporter, je les sacrifierais, à ce stade, pour au moins faire

political conversation and say, “Okay, we have our plan for the four sectors. What are we doing about health care? What are we doing about agriculture? What are we doing about personal car safety?”

It’s one thing to say that we’re going to ban Chinese electric vehicles because we’re worried about it, but I guarantee there are bigger problems across every car manufacturer that is connected to the internet right now.

We can’t have any of those conversations if we can’t even tie our shoes.

**Senator Richards:** At which stage would you say that national security is with this?

**Mr. Shipley:** We are at the whim of people who want to cause us harm. The only thing that keeps us safe right now is whether someone wants to take a swing at us. Our face is out there, and we’re going to take it on the nose.

**Senator Richards:** Thank you.

**Senator Batters:** First of all, I want to make a comment regarding this discussion in which we are saying, “Hurry up; get it done; it’s good enough; let’s get something done.” I agree that this is a very important topic, but the Senate has only had this bill for about two months, because we received it on the very last day we were sitting in June, and we started sitting again in September. Public consultations on this bill began as far back as 2016. It then took two years for this federal government to generate a national cybersecurity strategy, and then it took four years to introduce this bill and another two years to get to the Senate. It’s our job to make bills better than they are when we get them, so we should take a little bit of time to be able to do that properly.

In that regard, I’d like to ask Ms. Polsky from the Privacy and Access Council of Canada a question. When you referred to the proposed amendments to detail some of these very concerning issues — and I agree with you that some of them are very concerning — I’m assuming that that’s contained in here. I’d like to give you a bit of time to describe what you think are the two most important ones, if you had to narrow it down. I know it’s difficult to do, but if you have to do it, which ones would you focus on, and if you could describe for us and for Canadians how those could improve this bill.

avancer les choses et, je l’espère, faire avancer la conversation politique et dire : « D’accord, nous avons notre plan pour les quatre secteurs. Que faisons-nous pour les soins de santé? Que faisons-nous pour l’agriculture? Que faisons-nous en matière de sécurité automobile? »

C’est une chose de dire que nous allons interdire les véhicules électriques chinois parce que cela nous inquiète, mais je vous garantis qu’il y a des problèmes plus graves, chez tous les constructeurs automobiles, qui sont connectés à Internet en ce moment.

Nous ne pouvons avoir aucune de ces conversations si nous ne pouvons même pas lacer nos chaussures.

**Le sénateur Richards :** À quelle étape diriez-vous que la sécurité nationale se trouve dans cette affaire?

**M. Shipley :** Nous sommes à la merci de personnes qui veulent nous faire du mal. La seule chose qui nous protège en ce moment, c’est de savoir si quelqu’un veut s’en prendre à nous. Nous sommes une cible, et on ne nous manquera pas.

**Le sénateur Richards :** Merci.

**La sénatrice Batters :** Tout d’abord, j’aimerais faire une remarque concernant la discussion dans laquelle nous disons : « Dépêchons-nous, faisons-le, c’est déjà bien, faisons quelque chose. » Je reconnais qu’il s’agit d’un sujet très important, mais le Sénat n’a pas reçu ce projet de loi qu’il y a environ deux mois, puisque nous l’avons reçu à notre tout dernier jour de séance, en juin, et que nous avons recommencé à siéger en septembre. Les consultations publiques sur ce projet de loi remontent à 2016. Il a fallu ensuite deux ans au gouvernement fédéral pour élaborer une stratégie nationale de cybersécurité, puis quatre ans pour présenter ce projet de loi et encore deux ans pour qu’il arrive au Sénat. Il est de notre devoir de rendre les projets de loi meilleurs qu’ils ne le sont au moment où nous les recevons, et nous devrions donc prendre un peu de temps afin de le faire correctement.

À cet égard, j’aimerais poser une question à Mme Polsky, du Conseil du Canada de l’accès et la vie privée. Quand vous avez fait référence aux amendements proposés pour détailler certaines de ces questions très préoccupantes — et je suis d’accord avec vous pour dire que certaines sont très préoccupantes —, je suppose que c’est contenu dans la documentation. J’aimerais vous donner un peu de temps pour décrire les deux amendements que vous trouvez les plus importants, si vous deviez réduire la liste. Je sais que c’est difficile à faire, mais, si vous aviez à le faire, sur lesquels vous concentreriez-vous? Pourriez-vous aussi nous décrire et décrire aux Canadiens comment ces amendements pourraient améliorer le projet de loi?

**Ms. Polsky:** I'm sorry, I hate questions like that. We've narrowed it down to the top most important ones, and they are all important; it's a short list. Following from the previous question is on the consultation side.

At this point, to earn the public's trust to ensure that this piece of legislation actually does what it's designed and intended to do is to have a much more open consultation process as opposed to saying, "We consulted Canadians." Which ones?

We're not entitled to find out. Our government doesn't say these things. Allowing consultation, ensuring consultation with the requirement that the consultation results actually be considered and implemented as opposed to saying, "Thank you very much, we consulted; consultation ends today, and we're putting it in tomorrow." That's what we've seen until now.

Accountability and transparency are absolutely vital. We haven't had that until now. There's so much in this piece of legislation that is opaque and secret, and people are going to wonder why. We can look to the United States with the Foreign Intelligence Surveillance Act, or FISA, court orders — the secret orders — where people weren't allowed to contact a lawyer to say, "I received this order; what do I do?" because that was prohibited. We can't allow that level of secrecy. Whatever happened to open courts, regular rule of law and democratic processes? We don't know whom this shields, and that's part of the problem. It creates a shield against accountability, which will engender mistrust.

**Senator Batters:** I agree with you, and the issue of potentially secret courts, orders that defendants can't even know about or know what they might be facing, is something that I raised in my second reading speech about this bill. I'm the critic of the bill.

That's something I'd like you to explain a bit more for us. How would your amendments on that issue help to improve this bill?

**The Chair:** Sorry, Ms. Polsky. I hate to cut you off, but Senator Batters is out of time. If we have a chance to come back, we'll have an opportunity. If not, you might have to submit it in writing. I apologize.

**Senator McNair:** Thank you to the panellists for being here today and your testimony today in front of us. You've all made clear your views on whether the legislation should go forward or not.

**Mme Polsky :** Je suis désolée, je déteste ce genre de questions. Nous avons réduit la liste à ceux qui sont les plus importants, et ils sont tous importants; la liste est courte. La question précédente portait sur la consultation.

À ce stade, pour gagner la confiance du public et nous assurer que le projet de loi fait réellement ce qu'il est censé faire, il faut un processus de consultation beaucoup plus ouvert que celui qui consiste à dire : « Nous avons consulté les Canadiens. » Lesquels?

Nous n'avons pas le droit de le savoir. Notre gouvernement ne dit pas ces choses-là. Permettre la consultation, assurer qu'il y a des consultations en exigeant que ses résultats soient réellement pris en compte et mis en œuvre, plutôt que de dire : « Merci beaucoup, nous avons consulté; la consultation se termine aujourd'hui, et nous y donnerons suite demain. » C'est ce que nous avons vu jusqu'à présent.

La responsabilité et la transparence sont absolument essentielles. Nous n'en avons pas eu jusqu'à présent. Il y a tant de choses opaques et secrètes dans ce projet de loi que les gens vont se demander pourquoi. Il suffit de regarder ce qui se passe aux États-Unis avec les ordonnances judiciaires, secrètes, de la loi sur la surveillance des activités de renseignement, Foreign Intelligence Surveillance Act, qui interdisait à quiconque de contacter un avocat pour lui dire : « J'ai reçu une ordonnance judiciaire; que dois-je faire? ». Nous ne pouvons pas permettre un tel niveau de secret. Qu'est-il advenu de la transparence judiciaire, de la primauté du droit et des processus démocratiques? Nous ne savons pas qui cela protège, et c'est une partie du problème. Cela crée un bouclier contre la responsabilité, ce qui engendrera de la méfiance.

**La sénatrice Batters :** Je suis d'accord avec vous, et la question des tribunaux potentiellement secrets, des ordonnances dont les défendeurs ne peuvent même pas avoir connaissance et qui ne savent pas ce qui les attend, est un point que j'ai soulevé en deuxième lecture à propos de ce projet de loi. Je suis la critique de ce projet de loi.

C'est une chose que j'aimerais que vous nous expliquiez un peu plus. Comment vos amendements sur cette question contribueraient-ils à améliorer le projet de loi?

**Le président :** Désolé, madame Polsky, je dois vous interrompre, car le temps de la sénatrice Batters est écoulé. Si nous avons l'occasion d'y revenir, nous y reviendrons. Sinon, vous pourriez soumettre cela par écrit. Je vous prie de m'excuser.

**Le sénateur McNair :** Je remercie les témoins d'être présents aujourd'hui et d'avoir témoigné devant nous. Vous avez tous exprimé clairement votre point de vue sur l'opportunité d'adopter ou pas le projet de loi.

Mr. Warnell's comment was that this is a well-intentioned first step and that we're taking cybersecurity seriously. Two of you have mentioned the fact that we're not keeping up or we're lagging behind our Five Eyes allies. What's the impact of that? Do you see it getting to a point where they aren't going to be sharing information with us anymore if this legislation isn't passed as a first step?

**Mr. Warnell:** I'll share a point of view on that, senator, without any insider knowledge or perspective. I would argue that when one party in a group is not pulling its weight, they usually get left behind. I would expect that a similar behaviour or outcome could be facing Canada if we do not create the right tool and capabilities in our national law to be able to stay at least aligned with our most important allies.

Ideally, I'd like to see us leading the pack. We have amazing capabilities, leaders and technologists in the organizations that do this on a day-to-day basis on behalf of the Government of Canada. We need to be able to help them do their best, not only in Canada but for nations around the world.

**Mr. Shipley:** I think we don't necessarily risk the intelligence side, although I don't have specific expertise on that. My greatest thing is if you're the weakest kid in the group and someone wants to send a message, you're the kid that's going to get the beating. This is the risk that we run in terms of the schoolyard that are global affairs now and is going to be really brutal. I don't want to be that.

If you want to see what it looks like to be the squeaky toy of the Russians, look at what they did to Ukraine before they invaded. They crippled their power grid twice to 200,000 people in the winter to send a message. We're next if we don't get serious.

**Senator Dasko:** Thank you, witnesses. I have a follow-up on your comments, Mr. Shipley, about the lack of political will. Would you say that the fact that there is a bill indicates that there is political will?

**Mr. Shipley:** No. I will raise the point raised by a senator earlier about the time it takes a bill to get there. You saw political will with Bill C-70 on foreign interference. You saw the speed at which we finally oriented to the threat that we were taking seriously.

This bill is here through probably a lot of blood, sweat and tears from the people working behind the scenes to protect this country. It's here in spite of a largely political will, I feel, at this point. I would love to be wrong.

M. Warnell a déclaré qu'il s'agissait d'une première étape bien intentionnée et que nous prenions la cybersécurité au sérieux. Deux d'entre vous ont mentionné que nous ne sommes pas à la hauteur ou que nous sommes à la traîne par rapport à nos alliés du Groupe des cinq. Quel sera l'impact? Croyez-vous qu'ils en arriveront à ne plus partager d'information avec nous si ce projet de loi n'est pas adopté, dans un premier temps?

**M. Warnell :** Je vais vous faire part de mon point de vue à ce sujet, monsieur le sénateur, sans aucune connaissance ou perspective d'initié. Je dirais que, lorsqu'une partie d'un groupe ne fait pas sa part, elle est généralement laissée pour compte. Je crois qu'un comportement ou un résultat similaires attendent le Canada si nous ne créons pas les outils et les capacités adéquates dans notre législation nationale afin de rester au moins en phase avec nos alliés les plus importants.

Idéalement, j'aimerais nous voir en tête du peloton. Nous disposons de capacités, de dirigeants ou de technologues extraordinaires, dans les organisations qui travaillent au quotidien pour le gouvernement du Canada. Nous devons être en mesure de les aider à donner le meilleur d'eux-mêmes, non seulement au Canada, mais aussi dans les pays du monde entier.

**M. Shipley :** Je crois que nous ne mettons pas nécessairement en péril l'aspect du renseignement, mais je n'ai pas d'expertise spécifique en la matière. Ce qui m'importe le plus, c'est que, si vous êtes l'enfant le plus faible du groupe et que quelqu'un veut faire passer un message, c'est vous qui allez prendre les coups. C'est le risque que nous courons dans la cour d'école que sont aujourd'hui les affaires mondiales, et ce risque sera vraiment brutal. Je ne veux pas vivre cela.

Si vous voulez savoir à quoi cela ressemble d'être le jouet des Russes, regardez ce qu'ils ont fait à l'Ukraine avant de l'envahir. Ils ont paralysé deux fois le réseau électrique de 200 000 personnes, pendant l'hiver, afin de faire passer un message. Si nous n'agissons pas, nous serons les prochains.

**La sénatrice Dasko :** Merci à tous les témoins. J'aimerais revenir sur ce que vous avez dit à propos de l'absence de volonté politique, monsieur Shipley. Diriez-vous que le fait qu'il y a un projet de loi indique qu'il y a volonté politique?

**M. Shipley :** Non. Je mentionnerai le point soulevé par une sénatrice, tout à l'heure, concernant le temps qu'il faut pour qu'un projet de loi soit déposé. La volonté politique s'est manifestée avec le projet de loi C-70 sur l'ingérence étrangère. Vous avez vu à quelle vitesse nous nous sommes finalement intéressés à la menace, que nous prenions au sérieux.

Ce projet de loi est le fruit du sang, de la sueur et des larmes de ceux qui travaillent en coulisses pour protéger notre pays. Ce projet de loi est là en dépit d'une volonté essentiellement politique, me semble-t-il, à cette étape. J'aimerais avoir tort.

**Senator Dasko:** You spoke about the regulatory framework that's behind this and that lays down the road. Of course, with some bills, a lot of the regulatory work has already been done.

What is your perception of how much of that work is done? It may be the case that as soon as the bill it passed, the regulatory framework could be close behind, if I can put it that way. That is the case in some situations. In other situations, there is a lot of work left to be done. What is your sense of the work that's been done?

**Mr. Shipley:** From the conversations I have had with officials and others, I think our best-case scenario is within a year of Royal Assent that the regulation process could be done. I don't think it will be any faster than that. That means we have at least another year after the law passes before the regulations are finalized, and then whatever coming into force period may come in. We're still talking about two years from now, when there might be some accountability and additional tools to protect us. That is why my sense of urgency is so high, notwithstanding the flaws in the bill. We are still a year or two away from this actually meaning anything. That's where my perspective is on the time frame.

**Senator Dasko:** Mr. Warnell, Bruce Power obviously has very sophisticated systems already. Is this bill going to do anything or change anything that your company is doing?

**Mr. Warnell:** In respect to this bill, I think the nuclear industry in Canada is an indication of what "good" could look like. In fact, we've already been working for the better part of two decades hand-in-hand with our regulator, the Canadian Nuclear Safety Commission, with nuclear operators, with the nuclear supply chain partners, and with academics both internationally and within Canada to develop performance-based standards. We're fortunate that we are out-of-the-gate early, and we want to be there because it's the right thing to do and it's the safe thing to do.

This bill will have an impact on all industries. However, I think we are at a state of higher maturity to the ones that would be impacted the least from a degree of change. But we welcome the other industries that are both directly affected by this bill and those that we want to be effect through influence through the other critical infrastructure sectors to learn from what we've done, why we did it that way and why we believe it's an effective way to work forward on a safer Canada.

**Senator Dasko:** Basically your work is almost entirely done already.

**La sénatrice Dasko :** Vous avez parlé du cadre réglementaire qui sous-tend ce projet de loi et qui définit la voie à suivre. Bien entendu, pour certains projets de loi, une grande partie du travail réglementaire a déjà été effectuée.

Quelle est votre perception de l'ampleur de ce travail? Il est possible que, dès que le projet de loi sera adopté, le cadre réglementaire arrivera, si je peux le dire ainsi. C'est parfois le cas. D'autres fois, il reste beaucoup de travail à faire. Quelle est votre opinion sur le travail qui a été accompli?

**M. Shipley :** D'après les conversations que j'ai eues avec des responsables et d'autres personnes, je crois que, dans le meilleur des cas, le processus de réglementation pourrait être achevé dans l'année qui suit la sanction royale. Je ne crois pas que cela aille plus rapidement. Cela veut dire qu'il nous reste encore au moins un an, après l'adoption de la loi, avant que le règlement soit prêt, et qu'ensuite la période d'entrée en vigueur, quelle qu'elle soit, commence. Ce sera toujours de deux ans à partir de maintenant, quand il pourrait y avoir une certaine responsabilité ou des outils supplémentaires pour nous protéger. Voilà pourquoi je ressens une telle urgence, nonobstant les lacunes du projet de loi. Il faudra encore un an ou deux pour que cela signifie quelque chose. Voilà mon point de vue en ce qui concerne l'échéancier.

**La sénatrice Dasko :** Monsieur Warnell, Bruce Power dispose déjà, de toute évidence, de systèmes très sophistiqués. Ce projet de loi fera-t-il quelque chose ou changera-t-il quoi que ce soit à ce que fait votre entreprise?

**M. Warnell :** En ce qui concerne le projet de loi, je crois que l'industrie nucléaire au Canada est une indication de ce à quoi « bon » pourrait ressembler. D'ailleurs, nous travaillons déjà depuis près de 20 ans, en collaboration avec notre organisme de réglementation, la Commission canadienne de sûreté nucléaire, avec des exploitants nucléaires, des partenaires de la chaîne d'approvisionnement nucléaire et avec des chercheurs, tant au niveau international qu'au Canada, pour élaborer des normes axées sur le rendement. Nous avons la chance d'avoir commencé tôt, et nous voulons être là, car c'est la chose bonne et prudente à faire.

Ce projet de loi aura des répercussions sur toutes les industries. Cependant, je crois que nous avons atteint un niveau de maturité plus élevé que les industries qui seraient le moins affectées par un certain changement. Nous invitons les autres industries, celles directement touchées par ce projet de loi et celles que nous voulons influencer par le truchement des autres secteurs d'infrastructure critiques, à apprendre de ce que nous avons fait et des raisons pour lesquelles nous l'avons fait de cette manière et croyons que c'est une manière efficace de travailler vers un Canada plus sûr.

**La sénatrice Dasko :** En gros, vous avez déjà fait presque tout le travail que vous vouliez faire.

**Mr. Warnell:** I wish I could say that. The job we do is never done because the landscape and the threat is always changing.

Going back to one of the questions from a senator earlier, one of the primary critiques of this bill in its early stages is that it's very broad and wide. That is purposeful. I would expect the intention is not to trample civil liberties but to be quick to respond to a very fast-changing landscape and the threat dynamics that are changing hourly, daily and constantly. I have trust in Canadians at all levels of government, regulators, et cetera, to drive the right outcomes, and the broadness of the bill is actually the purpose to be able to respond. If you tried to regulate and legislate every scenario, every moment, we'll be talking about cybersecurity on Commodore 64s in 2032. It will take that long to get through the legislative process. The broadness is an important facet of enabling us to be a safer Canada.

**Senator Ross:** Mr. Shipley, you used the term "bare minimum" in your testimony. Mr. Warnell, you used the words "first steps." Could each of you suggest additional safeguards that could or should have been included in Bill C-26? What would they be?

**Mr. Warnell:** I'm happy to reiterate what I said in my opening comment about embracing and driving performance-based standards and not prescriptive standards. It's easy for someone to say that your should have a firewall in the regulations. If a firewall is no longer relevant two years from now, having that in the regulations because the law told us to do so is ineffective. Moving to performance-based, the organizations will take action to defend against this type of threat or that type of capability, and that will be changing over time. I would highly recommend that the language lean towards performance-based standards as it would serve Canadians well.

**Senator Ross:** Thank you.

**Mr. Shipley:** In terms of additional safeguards, I think Mr. Warnell said it very well. The breadth of this legislation enables the kind of flexible thinking we need to have. I wouldn't add anything else to this bill.

I would like to have narrowed the scope of individual accountability. I'm not in favour, in general, of piercing the corporate veil. We started down this road with the Canadian anti-spam legislation because there were known bad actors using corporate structures. I understand having the stick to drive compliance, but I don't necessarily believe it was warranted in this case or that it absolutely should be directed at people who

**M. Warnell :** J'aimerais pouvoir dire cela. Le travail que nous faisons n'est jamais réellement terminé, car le contexte et la menace changent toujours.

Pour revenir à l'une des questions posées par un sénateur, tout à l'heure, une des critiques principales formulées à l'encontre de ce projet de loi dans les premières étapes est qu'il est très large. C'est voulu. Je pense que l'intention n'est pas d'empiéter sur les libertés civiles, mais de pouvoir répondre rapidement dans un environnement qui évolue très rapidement et face à la dynamique des menaces qui change toutes les heures, tous les jours et constamment. Je fais confiance aux Canadiens de tous les ordres du gouvernement, organismes de réglementation, et cetera, pour obtenir les bons résultats, et la portée de ce projet de loi est en fait la portée voulue pour pouvoir réagir. Si vous essayez de réglementer et de légiférer chaque scénario, chaque moment, nous parlerons de la cybersécurité des Commodore 64 en 2032. Il faudra tout ce temps pour que le processus législatif aboutisse. L'ampleur de ce projet de loi est un aspect important, pour être un Canada plus sûr.

**La sénatrice Ross :** Monsieur Shipley, dans votre témoignage, vous avez utilisé le terme « strict minimum ». Monsieur Warnell, vous avez parlé de « premières étapes ». Pourriez-vous tous les deux proposer des mesures de protection supplémentaires qui pourraient ou auraient dû être incluses dans le projet de loi C-26? Quelles seraient-elles?

**M. Warnell :** Je suis heureux de répéter ce que j'ai dit dans mon commentaire d'ouverture sur le fait d'adopter et d'encourager des normes axées sur la performance et non pas des normes prescriptives. Il est facile de dire qu'il devrait y avoir une barrière de sécurité dans le règlement. Si cette barrière n'est plus pertinente deux ans plus tard, le fait qu'elle soit inscrite dans le règlement parce que la loi nous a dit de le faire est inefficace. En adoptant des normes axées sur la performance, les organisations prendront des mesures pour se défendre contre ce type de menace et ce type de capacité, qui changeront au fil du temps. Je recommande fortement que le libellé soit axé davantage sur les normes fondées sur la performance, car cela serait utile aux Canadiens.

**La sénatrice Ross :** Merci.

**M. Shipley :** Pour ce qui est des mesures de protection supplémentaires, je pense que M. Warnell l'a très bien exprimé. La portée de cette loi permet le type de réflexion souple que nous devons avoir. Je n'ajouterais rien d'autre au projet de loi.

J'aurais aimé que l'on réduise la portée de la responsabilité individuelle. En général, je ne suis pas en faveur de lever le voile sur les sociétés. Nous nous sommes engagés dans cette voie avec la Loi canadienne anti-pourriel, car nous savions que des mauvais acteurs utilisaient des structures organisationnelles. Je comprends que l'on veuille utiliser le bâton pour favoriser la conformité, mais je ne crois pas nécessairement que ce soit

are not directors of a company. I'm willing to let that one go and get dealt with in the future.

I still think it's profoundly unfair to small Canadian telecommunications carriers that through no fault of their own are told they have to get rid of their gear and they're stuck with the bill. I think there could have perhaps been a means-based approach or a fairness piece to that. But again, in the urgency — and I hear the senators' frustration — six years, which is ridiculous, to get this done, but now we're in a bad neighbourhood globally and we'd better get moving.

**Senator Ross:** Telecom companies here in Canada outsource a lot of their operations. It enables them to reduce some costs, but it also costs jobs in Canada. Can you speak to how this might threaten privacy protection, weaken telecommunications services or open ourselves up to cyber-threat?

**Ms. Polsky:** When your information is being accessed by someone in some other country and you have no recourse and no way of knowing even where it's being accessed, there are no controls. I appreciate it's to reduce costs, but at what cost? In this case, personal information. If that information is misappropriated and used for purposes that you really didn't intend — I was on the phone with my telecommunications carrier a few years ago, and they're in Singapore, and they said, don't worry, we have to abide by corporate polities. That was their justification. They knew they were golden because of corporate policies. I know they are frontline people, I don't expect them to know all of the laws, but they're using our information somewhere else.

When it comes to artificial intelligence and your calls are being recorded for training. These snippets are going to some other country where they're paid pennies to examine and help improve the AI. We have no control. When it comes to cybersecurity, that creates risk on an individual and, therefore, a national level. When we're looking at this piece of legislation that says carriers and others can be told to break encryption, that is a huge risk. Maybe it will be reasonably stated in the regulations as to why, when and under what circumstances encryption can be ordered to be broken. Perhaps very narrow circumstances can be prescribed, but from what we have seen in recent years, I'm not holding my breath.

**The Chair:** Thank you. We will have a last question.

justifié dans ce cas-ci ou que l'on doive absolument l'utiliser sur les personnes qui ne sont pas des administrateurs d'une entreprise. Je suis prêt à abandonner cet élément et à veiller à ce qu'on s'en occupe dans l'avenir.

Je pense toujours que c'est très injuste pour les petites entreprises canadiennes de télécommunications qui, sans que ce soit leur faute, se font dire qu'elles doivent se débarrasser de leur équipement et se retrouvent avec la facture. Je pense que l'on aurait dû adopter une approche axée sur les moyens ou faire preuve d'équité à cet égard. Mais encore une fois, dans l'urgence — et j'entends la frustration des sénateurs — six ans, ce qui est ridicule, pour faire avancer ce dossier... mais nous nous trouvons maintenant dans un mauvais voisinage à l'échelle mondiale et ferions mieux d'avancer.

**La sénatrice Ross :** Les entreprises de télécommunications au Canada confient en sous-traitance beaucoup de leurs activités. Cela leur permet de réduire certains coûts, mais cela coûte aussi des emplois au Canada. Pouvez-vous nous dire comment cette pratique pourrait menacer la protection de la vie privée, affaiblir les services de télécommunications ou nous exposer à des cybermenaces?

**Mme Polsky :** Lorsqu'une personne d'un autre pays accède à vos renseignements et que vous n'avez aucune ressource ni aucun moyen de savoir même à quoi elle accède, il n'y a pas de contrôles. Je reconnais que cela vise à réduire les coûts, mais à quel prix? Dans ce cas-ci, il s'agit des renseignements personnels. Si ces renseignements sont détournés et utilisés à des fins que vous n'aviez vraiment pas prévues... Il y a quelques années, j'étais au téléphone avec mon fournisseur de services de télécommunications, qui se trouve à Singapour, et il a dit, ne vous inquiétez pas, nous devons respecter les politiques d'entreprise. C'était sa justification. Il savait qu'il était protégé à cause des politiques organisationnelles. Je sais que ce sont des gens de première ligne. Je ne m'attends pas à ce qu'ils connaissent toutes les lois, mais ils utilisent nos renseignements ailleurs.

Pour ce qui est de l'intelligence artificielle et du fait que vos appels soient enregistrés à des fins de formation, ces extraits sont envoyés dans d'autres pays qui reçoivent des sous pour examiner et améliorer l'intelligence artificielle. Nous n'avons aucun contrôle. Pour ce qui est de la cybersécurité, cela crée un risque pour une personne et, ainsi, à l'échelle nationale. Quand ce texte de loi dit que les transporteurs et d'autres peuvent se faire demander de décrypter des données, c'est un énorme risque. Peut-être que le règlement énoncera raisonnablement pourquoi, quand et dans quelles circonstances on peut exiger le cryptage. Peut-être que l'on peut prescrire des circonstances très limitées, mais d'après ce que nous avons vu au cours des dernières années, je ne retiens pas mon souffle.

**Le président :** Merci. Nous aurons une dernière question.

**Senator Boehm:** Are you giving me the full four minutes?

**The Chair:** If you can keep it short, I would appreciate it.

**Senator Boehm:** All right, fine. Thank you.

Thank you witnesses for being here. My first question is for Ms. Polsky.

You know this very well, but privacy arrangements and regulations vary across various countries. There is always the challenge of getting the right alignment among countries. Generally speaking, I think the European Union's General Data Protection Regulation, or GDPR, is seen as the benchmark. In implementing regulations or just in the general implementation of Bill C-26, could there be a better alignment or continuous evergreen alignment with what other countries and organizations are doing?

**Ms. Polsky:** I think the provision is already there, whether it's in the Telecommunications Act, the Aeronautics Act or the Income Tax Act. Many of our federal laws already have language saying that the government can share our personal information with foreign governments, entities and individuals without notice or consent. Once "government 2.0" collects our information, under a number of laws, they can already export it and share it. There are international free-trade agreements that require information to be shared internationally.

As individuals, we have no way of knowing with whom our information is being shared and where it goes. We have no direct relationship with the ultimate recipient. We're helpless to do anything about it.

Regarding the GDPR, yes, when it was introduced in 2018, it quickly did become the global standard, but even with their form of consent and what we now have in Canadian legislation — which will be watered down if Bill C-27 passes — are all-or-nothing Faustian bargains. You consent to the collection, use and disclosure of your personal information with our partners and affiliates.

Who, where or for what? We don't have the ability to say, "Yes, share it, collect it and use for this purpose but not for that." That has to be strengthened and changed. Then, once encryption is protected in this and other laws and once the government is prohibited from operating in secret — years ago, Jean Chrétien said of Joe Clark that, "He should learn to do as I do and talk out of one side of his face." It was a wonderful quote, and it has been stuck in my brain since then. We have a government now that is

**Le sénateur Boehm :** M'accordez-vous les quatre minutes complètes?

**Le président :** Si vous pouvez être concis, je vous en serais reconnaissant.

**Le sénateur Boehm :** Très bien. Merci.

Je remercie les témoins d'être ici. Ma première question s'adresse à Mme Polsky.

Vous le savez très bien, mais les accords et les règlements sur la protection des renseignements personnels varient d'un pays à l'autre. Parvenir au bon alignement entre les pays pose toujours un défi. De manière générale, je pense que le Règlement général sur la protection des données de l'Union européenne, ou RGPD, est considéré comme le point de référence. Dans le cadre de la mise en œuvre du règlement ou simplement de la mise en œuvre générale du projet de loi C-26, pourrait-il y avoir un meilleur alignement ou un alignement continuel avec ce que les autres pays ou organisations font?

**Mme Polsky :** Je pense que la disposition est déjà là, qu'il s'agisse de la Loi sur les télécommunications, de la Loi sur l'aéronautique ou de la Loi de l'impôt sur le revenu. De nombreuses lois fédérales ont déjà un libellé disant que le gouvernement peut communiquer nos renseignements personnels aux particuliers, entités et gouvernements étrangers sans fournir de préavis ni obtenir de consentement. Une fois que le « gouvernement 2.0 » a recueilli nos renseignements, en vertu d'un certain nombre de lois, il peut déjà les exporter et les communiquer. Il existe des accords de libre-échange internationaux qui obligent la communication d'information à l'échelle internationale.

En tant que particuliers, nous n'avons aucun moyen de savoir avec qui nos renseignements sont échangés et à quel endroit ils sont envoyés. Nous n'avons aucune relation directe avec le destinataire ultime. Nous ne pouvons rien y faire.

En ce qui concerne le RGPD, oui, lorsqu'il est entré en vigueur en 2018, il est rapidement devenu la norme mondiale, mais même avec la forme de consentement prescrite et ce que prévoit déjà la législation canadienne — qui sera affaiblie si le projet de loi C-27 est adopté —, ce sont des pactes faustiens de type tout ou rien. Vous consentez à la collecte, à l'utilisation et à la communication de vos renseignements personnels avec nos partenaires et sociétés affiliées.

À qui sont-ils envoyés, où et pour quelle raison? Nous ne sommes pas en mesure de dire : « Oui, communiquez-les, recueillez-les et utilisez-les à cette fin, mais pas à celle-là. » C'est ce qui doit être renforcé et changé. Puis, une fois que le chiffrage sera protégé dans cette loi et dans d'autres et que le gouvernement se verra interdire d'agir en secret... Il y a quelques années, Jean Chrétien a dit de Joe Clark qu'« il devrait apprendre à faire ce que je fais et parler d'un côté de la bouche ». Cette

saying one thing and doing the other. That does not garner trust, it does not warrant trust and when it comes to national security and cybersecurity, it's a false foundation.

**Senator Boehm:** Thank you. Do I still have time for one question for Mr. Warnell?

**The Chair:** We're out of time. I would like you to ask your question, and we will have the panellist send their responses in writing so we'll have it for the record.

**Senator Boehm:** That's okay. I'll yield. It was a complicated one.

**The Chair:** I apologize, colleagues. We're out of time and we have to get to the next panel. I want to thank Ms. Polsky, Mr. Shipley and Mr. Warnell for taking the time to be with us here today. It's been very enriching. Thank you so much for being here.

For this next hour, we have the pleasure to welcome the Canadian Union of Public Employees, Brian Leclerc, Interim Chairperson, Provincial Council of the Communications Sector and Nathalie Blais, Research Representative. We also welcome from Electricity Canada, Francis Bradley, President and Chief Executive Officer, and from OpenMedia, by video conference, Matthew Hatfield, Executive Director.

I now invite to you provide opening remarks to be followed by questions from senators. You each have five minutes. I would welcome Mr. Leclerc to please begin.

[*Translation*]

**Brian Leclerc, Interim Chairperson, Provincial Council of the Communications Sector, Canadian Union of Public Employees:** Thank you, Mr. Chair. Thank you for inviting me to talk about outsourcing and offshoring telecommunications work. My name is Brian Leclerc, and I'm the interim chairperson of the Provincial Council of the Communications Sector of the Canadian Union of Public Employees, or CUPE, which represents some 6,000 telecommunications workers at Cogeco, Telus and Videotron in Quebec. Two of those companies, Telus and Videotron, have relocated thousands of jobs outside of Canada. Most of these jobs are in call centres, in technical support and various engineering positions. At Telus, approximately 7,000 jobs have been lost over the past decade in Canada. Over that same period of time, the total number of Telus employees abroad has quintupled and expanded to 37 countries, including India and the Philippines. Unfortunately, this phenomenon is showing no signs of slowing. In early 2024, Telus cut 175 jobs at CUPE alone.

citation magnifique est gravée dans mon esprit depuis. Nous avons maintenant un gouvernement qui dit une chose et fait le contraire. Cela ne suscite pas la confiance, ne justifie pas la confiance et, lorsqu'il s'agit de sécurité nationale et de cybersécurité, constitue une base erronée.

**Le sénateur Boehm :** Merci. Me reste-t-il du temps pour poser une question à M. Warnell?

**Le président :** Le temps est écoulé. J'aimerais que vous posiez votre question, et nous demanderons à l'intervenant d'envoyer ses réponses par écrit, pour que cela soit dans le compte rendu.

**Le sénateur Boehm :** C'est bon. Je vais céder la parole. C'était une question compliquée.

**Le président :** Je suis désolé, chers collègues. Nous sommes à court de temps et devons passer au prochain groupe de témoins. Je veux remercier Mme Polsky, M. Shipley et M. Warnell d'avoir pris le temps d'être avec nous ici aujourd'hui. La discussion a été très enrichissante. Merci beaucoup de votre présence ici.

Pour la prochaine heure, nous avons le plaisir d'accueillir Brian Leclerc, président par intérim, Conseil provincial du secteur des communications, et Nathalie Blais, conseillère à la recherche, du Syndicat canadien de la fonction publique. Nous recevons également Francis Bradley, président et chef de la direction d'Électricité Canada, et Matthew Hatfield, directeur exécutif d'OpenMedia, par vidéoconférence.

Je vous invite maintenant à présenter vos déclarations liminaires qui seront suivies par les questions des sénateurs. Vous aurez chacun cinq minutes. Je demande à M. Leclerc de bien vouloir commencer.

[*Français*]

**Brian Leclerc, président par intérim, Conseil provincial du secteur des communications, Syndicat canadien de la fonction publique :** Merci, monsieur le président. Je vous remercie de m'avoir invité à parler de la sous-traitance et du déplacement du travail des télécommunications à l'étranger. Mon nom est Brian Leclerc et je suis président par intérim du Conseil provincial du secteur des communications au Syndicat canadien de la fonction publique (SCFP), qui représente environ 6 000 travailleuses et travailleurs des télécommunications au sein de Cogeco, Telus et Vidéotron au Québec. Deux de ces compagnies, soit Telus et Vidéotron, délocalisent des milliers d'emplois à l'extérieur du Canada. Il s'agit principalement de postes dans des centres d'appels, dans le soutien technique et différentes fonctions d'ingénierie. Chez Telus, ce sont près de 7 000 emplois syndiqués qui ont été perdus depuis 10 ans au Canada. Pendant la même période, le nombre total de travailleurs de Telus a quintuplé à l'étranger et s'est étendu à 37 pays, dont l'Inde et les Philippines. C'est une situation qui,

Videotron is outsourcing customer service work to Egypt, Morocco, Romania and Senegal, where wages are much lower than they are here. Relocating jobs abroad violates the Telecommunications Act, which is intended to develop a system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions.

This is also a business model that we feel conflicts with other objectives set out in the bill, such as ensuring the safety of Canadian telecommunications networks and protecting privacy. Outsourcing telecommunications work may also pose a national security threat for several reasons. First, Canadians' personal information gets out more. More people in a number of other countries have access to that information. Meanwhile, Canada has strained relationships with a growing number of states, including India, Russia and China. Even if we could be absolutely sure that client files are stored on servers located in Canada, personal information is still being made available outside the country, and that makes recourse in the case of a data breach complicated. Some Telus employees actually testified that their personal information was stolen in February 2023.

A few months later, the unions learned that our pay management system had been transferred to the Philippines, and we're still waiting on the outcome of that investigation. In Egypt and Morocco, Telecom Egypt, an Egyptian-owned entity, operates the Xceed call centres, which are Videotron subcontractors. People make a big deal out of TikTok, which allowed the Chinese government to get its hands on our personal information through its app, but the situation in Egypt isn't much different. However, it is less known and more worrisome because call centres have access to sensitive information that could enable the state to target devices, access protected systems or carry out massive attacks.

Skilled telecom jobs are also being outsourced. These are jobs in technology architecture, engineering and design. These jobs can provide access to very sensitive information, such as IP address blocks, the internal network architecture of commercial clients in Canada and the location of certain strategic components of Canadian telecommunications networks. All this information can be used by bad actors to harm Canada's economy and democracy.

malheureusement, est loin de s'essouffler, car depuis le début de l'année 2024, Telus a supprimé 175 postes au SCFP seulement.

Chez Vidéotron, on externalise du travail de service à la clientèle en Égypte, au Maroc, en Roumanie et au Sénégal, où les salaires sont beaucoup plus faibles qu'ici. La délocalisation des emplois à l'étranger entre en contradiction avec la Loi sur les télécommunications, qui vise à favoriser le développement d'un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions.

C'est aussi un modèle d'affaires qui, à notre avis, va à l'encontre d'autres objectifs de la loi, qui sont la sûreté des réseaux de télécommunication canadiens et la protection de la vie privée. Le déplacement du travail de télécommunication à l'extérieur de nos frontières peut également représenter une menace à la sécurité nationale pour plusieurs raisons. Tout d'abord, les renseignements personnels des Canadiens voyagent davantage. Or, un plus grand nombre de personnes y ont accès dans plusieurs pays, alors que le Canada a des relations tendues avec un nombre croissant d'États, dont l'Inde, la Russie et la Chine. Même si l'on avait la certitude que les dossiers des clients sont conservés sur des serveurs situés au Canada, il n'en demeure pas moins qu'on rend des informations personnelles disponibles à l'extérieur du pays, ce qui complique tout recours en cas de fuite des données. Certains employés de Telus eux-mêmes ont fait des témoignages sur le vol de leurs renseignements personnels en février 2023.

Quelques mois plus tard, les syndicats apprenaient que le système de gestion de nos paies était transféré aux Philippines, et le résultat de l'enquête se fait toujours attendre. En Égypte et au Maroc, c'est Telecom Egypt, propriété du gouvernement égyptien, qui exploite les centres d'appels Xceed, sous-traitant de Vidéotron. On a fait grand cas de TikTok, qui permettait au gouvernement chinois de mettre la main sur nos renseignements personnels grâce à son application, mais la situation en Égypte n'est pas très différente. Elle est, par contre, méconnue et plus inquiétante, puisque les centres d'appels ont accès à des données sensibles qui pourraient permettre à l'État de cibler des appareils, d'accéder à des systèmes protégés ou de mener des attaques massives.

Les emplois spécialisés en télécommunication sont aussi externalisés; on parle ici de postes en architecture technologique, en ingénierie ou en dessin de plan. Ce sont des postes qui peuvent donner accès à des informations très sensibles, comme des blocs d'adresses IP, l'architecture de réseau interne des clients commerciaux au Canada et la localisation de certaines composantes stratégiques des réseaux de télécommunication canadiens. Tous ces renseignements pourraient être utilisés par des acteurs malveillants pour faire mal à l'économie ou à la démocratie canadienne.

Relocating telecommunications jobs abroad can jeopardize national security. The government needs to make sure it has the legislative tools to put an end to that because it's a weak link in Canada's telecommunications system. We urge the committee to get out in front of this and amend Bill C-26 by adding an objective to the Telecommunications Act, whereby relocating and subcontracting our jobs abroad is forbidden. That would make it clear that the CRTC has the power to monitor jobs and require all personnel directly and indirectly involved in operating telecommunications networks to remain in Canada.

We also urge the committee to add a whistle-blower protection measure to Bill C-26 to enhance the ability to detect threats to Canadian telecommunications systems. Thank you for your attention.

[*English*]

**The Chair:** Thank you.

**Francis Bradley, President and Chief Executive Officer, Electricity Canada:** It's a pleasure once again to have the honour to meet with this committee.

[*Translation*]

I am the president of Electricity Canada, the voice for Canadian electricity. Our members produce, transport and distribute electricity to every Canadian province and territory. Today, my remarks will focus on part 2 of the bill, the critical cyber systems protection act.

[*English*]

Before I proceed, I want to recognize the efforts made by the House of Commons Standing Committee on Public Safety and National Security who made several amendments in line with our recommendations. These include, one, adding the "consistency with regulatory regimes" clause, aiding alignment with existing frameworks and upcoming regulations; two, allowing the incident reporting period to be defined through regulations instead of fixed in the legislation, ensuring adequate flexibility; and three, enhancing transparency through additional ministerial reporting requirements to Parliament.

Now while these are positive steps, two critical recommendations were made.

First, the bill must align with existing regulatory frameworks. While the addition of the "consistency with regulatory regimes"

La sécurité nationale peut être menacée par le déplacement de postes de télécommunication à l'extérieur de nos frontières. Il est impératif que le gouvernement se dote d'outils législatifs qui pourront y mettre un terme, car il s'agit du maillon faible des télécommunications au Canada. Nous proposons donc au comité d'agir en amont et d'amender le projet de loi C-26 pour ajouter un objectif à la Loi sur les télécommunications visant à interdire le déplacement ou la sous-traitance de nos emplois à l'étranger. De cette façon, il serait clair que le CRTC a le pouvoir d'effectuer une surveillance de l'emploi et d'exiger le maintien au Canada de l'ensemble du personnel lié de près ou de loin à l'exploitation des réseaux de télécommunication.

Nous suggérons également au comité d'ajouter une mesure de protection des lanceurs d'alerte au projet de loi C-26 afin d'améliorer la capacité de détection des menaces qui visent les systèmes canadiens de télécommunication. Je vous remercie de votre attention.

[*Traduction*]

**Le président :** Merci.

**Francis Bradley, président et chef de la direction, Électricité Canada :** Je suis ravi d'avoir une fois de plus l'honneur de rencontrer le comité.

[*Français*]

Je suis président d'Électricité Canada. C'est une association qui est la voie de l'électricité au Canada; nos membres produisent, transportent et distribuent de l'électricité dans chaque province et territoire du Canada. Mes commentaires aujourd'hui se concentreront sur la partie 2 du projet de loi, la Loi sur la protection des cybersystèmes essentiels.

[*Traduction*]

Tout d'abord, je tiens à souligner les efforts du Comité permanent de la sécurité publique et nationale de la Chambre des communes, qui a proposé plusieurs amendements conformes à nos recommandations. Il s'agit, premièrement, d'ajouter la disposition sur la « compatibilité avec les régimes de réglementation », ce qui contribue à l'alignement avec les cadres existants et les règlements à venir; deuxièmement, de permettre que la période de signalement des incidents soit définie dans les règlements plutôt que fixés dans la loi, ce qui garantit une flexibilité adéquate; et troisièmement, de rehausser la transparence en ajoutant des obligations pour le ministre de rendre compte au Parlement.

Bien qu'il s'agisse de mesures positives, nous avons formulé deux recommandations essentielles.

Premièrement, le projet de loi doit s'aligner sur les cadres réglementaires existants. Même si l'ajout de la « compatibilité

clause is a step in the right direction, it is insufficient to address our sector's specific concerns.

The electricity sector is unique in that it is regulated already under the North American Electric Reliability Corporation's, or NERC's critical infrastructure protection standards. These standards, which have been adopted, enforced and audited by provincial regulators, ensure robust measures to secure the grid. Introducing new requirements under Bill C-26 risks regulatory conflicts, compliance burdens and ambiguity, undermining the bill's goal, the goal of enhancing system safety.

A risk-based approach is essential. By imposing fewer requirements on mature operators with strong cybersecurity programs, resources can be focused on incident prevention rather than additional compliance. Regulators in turn can prioritize high-risk operations or sectors.

Second, safe harbour provisions should be established to grant legal protections to operators who share information with government agencies. The electricity sector maintains a collaborative and strong relationship with Communications Security Establishment Canada, openly sharing information to enhance grid security. Mandatory reporting requirements under Bill C-26 could jeopardize this relationship unless safeguards are established.

The inclusion of safe harbour provisions encourages timely and open information sharing between industry and government without the risk of liability. Similar measures have been adopted in the United States with the passage of the Cyber Incident Reporting for Critical Infrastructure Act.

Imposing mandatory requirements may also create a chilling effect on the industry's relationship with government departments and agencies. Without appropriate safeguards, operators will likely receive legal advice to share just enough information to comply with the act and nothing more.

This is counterproductive to the goals of the legislation, but there are a couple of things you can do to mitigate those risks. For a start, the legislation should explicitly clarify that information shared voluntarily with CSE outside of legislative or regulatory requirements imposed by Bill C-26 will not be shared with the regulator or enforcement agencies. Critical infrastructure operators currently enjoy a collaborative relationship with the CSEs Centre for Cyber Security. This is

avec les régimes de réglementation » constitue un pas dans la bonne direction, il ne suffit pas pour réagir aux préoccupations particulières de notre secteur.

Le secteur de l'électricité est unique, en ce sens qu'il est déjà réglementé en vertu des normes de protection des infrastructures essentielles de la North American Electric Reliability Corporation, ou NERC. Ces normes, qui ont été adoptées, appliquées et vérifiées par les organismes de réglementation provinciaux, garantissent la prise de mesures robustes pour sécuriser le réseau. L'introduction de nouvelles exigences en vertu du projet de loi C-26 risque d'entraîner des conflits réglementaires, des fardeaux liés au respect de la conformité et une ambiguïté, ce qui mine l'objectif du projet de loi, qui est de renforcer la sécurité des systèmes.

Il faut adopter une approche axée sur le risque. En imposant moins d'exigences à des exploitants matures dotés de robustes programmes de cybersécurité, on peut concentrer les ressources sur la prévention des incidents plutôt que sur des mesures de conformité supplémentaires. Les organismes de réglementation peuvent à leur tour accorder la priorité aux opérations ou aux secteurs à risque élevé.

Ensuite, il faut établir des dispositions d'exonération pour accorder des protections juridiques aux exploitants qui communiquent des renseignements aux agences gouvernementales. Le secteur de l'électricité entretient une solide relation de collaboration avec le Centre de la sécurité des télécommunications Canada, en communiquant ouvertement des renseignements afin de renforcer la sécurité des réseaux. Les exigences de signalement obligatoires prévues dans le projet de loi C-26 pourraient mettre en péril cette relation, à moins que des mesures de protection ne soient établies.

L'inclusion de dispositions d'exonération encourage la communication d'information opportune et ouverte entre l'industrie et le gouvernement sans risque de responsabilité. Des mesures similaires ont été adoptées aux États-Unis dans le cadre de l'adoption de la Cyber Incident Reporting for Critical Infrastructure Act.

Imposer des exigences obligatoires pourrait également refroidir la relation de l'industrie avec les ministères et organismes gouvernementaux. Sans mesures de protection appropriées, les exploitants recevront probablement des conseils juridiques leur permettant de communiquer juste assez d'information pour se conformer à la loi, sans plus.

Cela va à l'encontre des objectifs de la loi, mais il y a deux ou trois choses à faire pour atténuer ces risques. D'abord, la loi doit explicitement clarifier que les renseignements échangés volontairement avec le CST à l'extérieur des obligations législatives ou réglementaires imposées par le projet de loi C-26 ne seront pas communiqués à l'organisme de réglementation ou aux agences d'application de la loi. Les exploitants d'infrastructures essentielles entretiennent actuellement une

grounded in the confidence that the Cyber Centre does not disclose operator's information to regulators, enforcement agencies or other departments. Protecting the Cyber Centre from any additional information sharing obligations is crucial to maintaining this collaborative relationship.

A similar relationship exists between NERC and the Electricity Information Sharing and Analysis Centre, to which electricity operators voluntarily share information about cyber and physical incidents. While the E-ISAC is operated by NERC, it is organizationally isolated from its enforcement processes, ensuring confidentiality and fostering open information exchange with electricity operators.

[*Translation*]

Although many other aspects of the bill also deserve our attention, that's all the time I have for today. I would encourage you to consult our brief, which contains more recommendations for improving the bill. Thank you.

[*English*]

**The Chair:** Thank you, Mr. Bradley. Our final witness for this panel is Matthew Hadfield from OpenMedia.

**Matthew Hatfield, Executive Director, OpenMedia:** Good evening, I'm Matt Hatfield, the executive director of OpenMedia, a non-partisan, grassroots community of over 250,000 people in Canada who work for an open, affordable and surveillance-free internet. I'm speaking to you from the unceded territory of the Sto:lo, Tsleil-Waututh, Squamish and Musqueam nations.

Bill C-26 is not yet fit for service, period. I am hoping you give yourselves the time it will take to fix it. For ordinary Canadians, cybersecurity is inseparable from privacy, whether you are a hockey dad, a business owner or a Canadian senator, none of us wants the details of our lives spied on, by hackers, a hostile state or our own government. We all want private lives to stay private. That's a cornerstone of democracy and a fundamental human need.

That is why since its inception, Bill C-26 has caused alarm for folks in OpenMedia's community. We absolutely need stronger cybersecurity, but nobody is going to trust a cybersecurity framework that threatens our personal privacy. Cybersecurity and privacy must go hand-in-hand.

relation de collaboration avec le Centre pour la cybersécurité du CST. Elle repose sur la confiance que le Centre pour la cybersécurité ne divulgue pas les renseignements de l'exploitant aux organismes de réglementation, aux agences d'application de la loi ou à d'autres ministères. La protection du Centre pour la cybersécurité contre toutes obligations supplémentaires d'échange de renseignements est essentielle pour maintenir cette relation de collaboration.

Il existe une relation similaire entre le NERC et l'Electricity Information Sharing and Analysis Centre, à qui les exploitants de réseau communiquent volontairement de l'information au sujet des cyberincidents et des incidents physiques. Bien que l'E-ISAC soit exploité par le NERC, son organisation est isolée de ses processus d'application de la loi, ce qui garantit la confidentialité et renforce l'échange de renseignements ouvert avec les exploitants de réseau.

[*Français*]

Bien que de nombreux autres aspects du projet de loi méritent également qu'on leur porte attention, c'est tout le temps dont je dispose aujourd'hui, mais je vous encourage à consulter notre mémoire, qui contient d'autres recommandations sur la manière d'améliorer le projet de loi. Merci.

[*Traduction*]

**Le président :** Merci, monsieur Bradley. Notre dernier témoin de ce groupe est Matthew Hadfield, d'OpenMedia.

**Matthew Hatfield, directeur exécutif, OpenMedia :** Bonsoir. Je suis Matthew Hatfield, directeur exécutif d'OpenMedia, un regroupement communautaire non partisan de plus de 250 000 personnes au Canada qui travaillent pour un Internet ouvert, abordable et exempt de surveillance. Je m'adresse à vous depuis le territoire non cédé des nations Sto:lo, Tsleil-Waututh, Squamish et Musqueam.

Le projet de loi C-26 n'est pas encore en état de servir, un point c'est tout. J'espère que vous vous donnerez le temps nécessaire pour le corriger. Pour les Canadiens ordinaires, la cybersécurité est indissociable de la protection de la vie privée. Que vous soyez papa de hockey, propriétaire d'entreprise ou sénateur canadien, personne d'entre nous ne veut que les détails de notre vie ne soient espionnés par des pirates, un État hostile ou notre propre gouvernement. Nous voulons tous que notre vie privée demeure privée. C'est la pierre angulaire de la démocratie et un besoin humain fondamental.

C'est pourquoi, depuis ses débuts, le projet de loi C-26 a suscité l'inquiétude de la communauté d'OpenMedia. Nous avons absolument besoin d'une cybersécurité plus solide, mais personne n'aura confiance en un cadre de cybersécurité qui menace notre vie personnelle. La cybersécurité et la vie privée doivent aller de pair.

Regular Canadians do want and value cybersecurity. Cyber-threats that touch our lives are growing daily, with many emanating from hostile states no friend to democracies. Canada has not been defending ourselves adequately from these threats, and that has to change. Bill C-26's goal is commendable, but the means by which it is currently seeking to achieve this goal, through granting the government sweeping new powers to obtain our private information without careful checks and balances, is not.

Here is where I have to blunt: People do not trust the government when it says it only wants our private information to protect us. Rightly so. People do not want the government to have inspection powers at will to access our private lives. People want our private lives kept private, and that means kept private from both hostile states and our own government. This is not about whether we trust Justin Trudeau or Pierre Poilievre or the NDP or the Bloc Quebecois. This is about who we are as Canadians, and the kind of society we want to live in.

As things stand, people cannot trust Bill C-26. Yes, it was improved by MPs in its journey through the House of Commons, but it contains several ticking time bombs that may severely hurt Canadians in the future if you don't fix them.

Time bomb number one is that Bill C-26 allows the government to keep its orders to telecoms entirely secret and indefinitely. We all understand the need to, at times, act quickly and conceal parts of decisions from Canada's adversaries, but permanent secrecy without mandated disclosure is extremely dangerous. If this section is not fixed, we are laying the foundation for a vast and growing secret governance and surveillance architecture created by these orders that do not belong in additional democracy.

Time bomb number two is that Bill C-26 gives the government far too free a hand to order telecoms, banks and other designated institutions to hand over our private, personal information and use and share that information as it chooses, including with foreign entities. Canadians should have confidence that information collected for cybersecurity is used for that purpose alone, and not to trawl for signs of protest activity or to be given freely to law enforcement. Right now, that confidence simply isn't there.

Les Canadiens ordinaires veulent et valorisent la cybersécurité. Les cybermenaces qui touchent notre vie augmentent chaque jour, et un grand nombre d'entre elles proviennent d'États hostiles qui ne sont pas favorables aux démocraties. Le Canada ne s'est pas bien défendu contre ces menaces, et cela doit changer. L'objectif du projet de loi C-26 est louable, mais les moyens par lesquels il cherche actuellement à atteindre cet objectif, en accordant au gouvernement de nouveaux pouvoirs radicaux pour obtenir nos renseignements privés sans freins et contrepoids prudents, ne l'est pas.

C'est ici que je dois être direct : les gens ne font pas confiance au gouvernement lorsqu'il dit qu'il veut nos renseignements privés uniquement afin de nous protéger. Et ils ont raison. Les gens ne veulent pas que le gouvernement dispose de pouvoirs d'inspection à sa guise pour accéder à leur vie privée. Ils veulent que leur vie privée reste privée, ce qui signifie qu'elle doit être protégée à la fois des États hostiles et de notre propre gouvernement. Il ne s'agit pas de savoir si nous faisons confiance à Justin Trudeau, à Pierre Poilievre, au NPD ou au Bloc Québécois. Il s'agit de savoir qui nous sommes en tant que Canadiens et le type de société dans laquelle nous voulons vivre.

Dans l'état actuel des choses, les gens ne peuvent pas avoir confiance dans le projet de loi C-26. Oui, il a été amélioré par les députés lorsqu'il est passé par la Chambre des communes, mais il contient plusieurs bombes à retardement qui, si vous ne les désamorcez pas, peuvent causer un préjudice grave aux Canadiens dans l'avenir.

La première bombe à retardement est que le projet de loi C-26 permet au gouvernement de garder ses décrets à l'intention des entreprises de télécommunications entièrement secrets, et ce, indéfiniment. Nous comprenons tous la nécessité, parfois, d'agir rapidement et de dissimuler des parties de décisions à des adversaires du Canada, mais le secret permanent sans divulgation imposée est extrêmement dangereux. Si cet article n'est pas modifié, nous jetons les bases d'une vaste architecture de gouvernance et de surveillance de plus en plus secrète créée par ces décrets qui n'ont pas leur place dans une démocratie supplémentaire.

La deuxième bombe à retardement est que le projet de loi C-26 donne au gouvernement une marge de manœuvre beaucoup trop grande pour ordonner aux entreprises de télécommunications, aux banques et à d'autres institutions désignées de céder nos renseignements personnels et privés, de les utiliser et de les communiquer comme bon lui semble, y compris à des entités étrangères. Les Canadiens devraient être convaincus que les renseignements recueillis à des fins de cybersécurité sont utilisés à cette seule fin, et non pas pour recueillir des signaux d'activités de manifestation ou pour qu'ils soient donnés librement à des organismes d'application de la loi. En ce moment, cette confiance n'est tout simplement pas là.

Time bomb number three is that Bill C-26 continues to give the government the power to install the devices on networks that break encryption. Forbidding the minister from directly demanding our private messages without additional safeguards is like saying Bill C-26 doesn't require that we report our conversations directly to the government, only that we keep a government phone in the room and off the hook everywhere we go.

Alongside many other civil society organizations and experts, OpenMedia has delivered a brief to you with common sense, straightforward amendments that would forbid the government from ordering the compromising of encryption, ensure government orders cannot stay secret indefinitely without judicial oversight, and ensure our personal information gathered under Bill C-26 is used only for cybersecurity purposes.

As many experts both here and in the House of Commons have testified, cybersecurity needs to be a team sport. Everyone needs to be on board for it to work, yet we're living in a period of fracturing social trust. If we allow Bill C-26 to pass riddled with clear privacy and secrecy problems, we will be contributing to that decline in trust and undermining privacy, security and Canadian democracy.

Nearly 14,000 messages were sent by OpenMedia to the House of Commons asking them to fix Bill C-26. Today, their eyes are on you to finish the job. As senators, you have a vital constitutional duty to fix Bill C-26 and make it legislation all Canadians can have confidence in. Thank you, and I look forward to your questions.

**The Chair:** Thank you, Mr. Hatfield. We will now proceed to questions. As usual, four minutes will be allocated to each question, including the answer. I ask that you keep your questions succinct in an effort to allow as many interventions as possible. The first question goes to the deputy chair, Senator Dagenais.

[*Translation*]

**Senator Dagenais:** My first question is for Mr. Leclerc. I'm astounded that telecommunications companies are unable to set up firewalls to control access to personal information. If that's true, I find that very worrisome. Can you give us examples of the risks that employees based in other countries pose to customers of telecommunications companies? How can that happen?

La troisième bombe à retardement est que le projet de loi C-26 continue de donner au gouvernement le pouvoir d'installer les appareils sur des réseaux qui permettent de déchiffrer le cryptage. Interdire au ministre d'exiger directement nos messages privés sans mesures de protection supplémentaires revient à dire que le projet de loi C-26 ne nous oblige pas à rapporter nos conversations directement au gouvernement, mais seulement à garder décroché partout où nous allons un téléphone du gouvernement.

À côté de nombre d'organisations de la société civile et d'experts, OpenMedia vous a présenté un mémoire qui contient des amendements sensés et directs qui interdiraient au gouvernement d'ordonner la compromission du cryptage, de s'assurer que les décrets gouvernementaux ne peuvent pas rester secrets indéfiniment sans surveillance judiciaire, et de veiller à ce que nos renseignements personnels recueillis en vertu du projet de loi C-26 ne soient utilisés qu'à des fins de cybersécurité.

Comme l'ont déclaré de nombreux experts ici et à la Chambre des communes, la cybersécurité doit être un travail d'équipe. Tout le monde doit y adhérer pour qu'elle fonctionne, or nous vivons dans une période de fracture de la confiance sociale. Si nous permettons que le projet de loi C-26 soit adopté avec de nombreux problèmes clairs en matière de protection des renseignements personnels et de confidentialité, nous contribuerons à ce déclin de la confiance et à miner la vie privée, la sécurité et la démocratie canadienne.

OpenMedia a envoyé à la Chambre des communes près de 14 000 messages pour lui demander de corriger le projet de loi C-26. Aujourd'hui, il compte sur vous pour terminer le travail. En tant que sénateurs, vous avez une obligation constitutionnelle essentielle de corriger le projet de loi C-26 et d'en faire une loi en laquelle tous les Canadiens auront confiance. Je vous remercie, et je suis impatient de répondre à vos questions.

**Le président :** Merci, monsieur Hatfield. Nous allons maintenant passer aux questions. Comme à l'habitude, il y aura quatre minutes pour chaque question, y compris la réponse. Je vous demande de bien vouloir garder vos questions succinctes afin de permettre le plus grand nombre d'interventions possible. La première question revient au vice-président, le sénateur Dagenais.

[*Français*]

**Le sénateur Dagenais :** Ma première question s'adresse à M. Leclerc. Je suis étonné que les entreprises de télécommunication ne soient pas en mesure d'établir des coupe-feu pour contrôler l'accès aux données personnelles. Si c'est le cas, je vous dirais que c'est plutôt inquiétant. Pouvez-vous nous donner des exemples des risques que les employés qui sont à l'étranger représentent pour la clientèle des entreprises de télécommunication? Comment cela peut-il se passer?

**Mr. Leclerc:** It happens in a number of different ways. When I was hired by my employer, I had to go through a criminal record check. Do they do that in other countries? Who knows? They have access to all the information in our accounts, in the network infrastructure. I mentioned that in my opening remarks. If some entity or a disgruntled, underpaid employee who is seeking revenge or wants to send a message gets their hands on IP addresses, that introduces a lot of vulnerability.

The previous panel of witnesses made that clear, too. We're very vulnerable to all kinds of attacks.

**Senator Dagenais:** Thank you. Mr. Bradley, my next question is for you. I'm looking at the members of your organization, such as Hydro One, Hydro-Québec, major provincial corporations and cities, including smaller ones, that have their own electric utility for their residents. Not all those entities have the same revenue and the same resources.

Considering those differences, do you think all these corporations have sufficiently reassuring capacity to fight cyberattacks? If not, are some of them — not naming names — more vulnerable to attack?

[*English*]

**Mr. Bradley:** That is an excellent question, and one that is often asked of the sector. As you point out, there is a significant difference in terms of the size of the largest of our companies to the smallest companies. Our focus — and it is also the focus of the North American Electric Reliability Corporation — tends to be, principally those companies that are a part of the bulk power system. Any company that is interconnected and is interconnected at a kind of transmission level where the impacts of a breach would potentially cascade.

We work with our smallest members to help them with everything from cyber-hygiene to best practices and information sharing. But the principal focus of the association and the North American effort in this space has always been to ensure that everyone who is involved in the bulk electric power system in North America is at a security level that is more than sufficient.

Our concern for a number of years, long before this legislation ever became drafted — and I've been part of these discussions for almost 20 years in terms of what the legislative frameworks will be — our concern has always been that we have an electricity sector that we think is quite mature in terms of its approach, but my biggest concern is all the interdependencies. My concern is not necessarily with my smaller members; my concern is with the other sectors which we depend on whether it's telecommunications, finance, water or transportation.

**M. Leclerc :** Cela peut se passer de multiples manières. Lorsque j'ai été embauché par mon employeur, j'ai subi une vérification de mes antécédents judiciaires. Font-ils cela à l'étranger? On ne le sait pas. Ils ont accès à l'ensemble des données que nous avons dans nos comptes, dans l'infrastructure réseau. Je l'ai mentionné dans mon allocution d'ouverture. Si les adresses IP tombent entre les mains d'un élément ou d'un employé qui se considère comme lésé, mal payé, qui veut se venger ou envoyer un message, on est alors très vulnérable.

Le groupe de témoins précédent l'a clairement montré aussi. Nous sommes très vulnérables à toutes sortes de tentatives.

**Le sénateur Dagenais :** Je vous remercie. Monsieur Bradley, ma prochaine question s'adresse à vous. Je regarde qui sont les membres de votre organisation, par exemple Hydro One, Hydro-Québec, de grandes sociétés provinciales et des villes parfois petites qui ont leur propre service d'électricité pour leurs citoyens. Tout ce monde-là n'a pas les mêmes revenus ni les mêmes ressources.

En tenant compte de leurs différences, pensez-vous que toutes ces sociétés ont des capacités minimales et suffisamment rassurantes pour lutter contre les cyberattaques? Sinon, y en a-t-il, sans vouloir les nommer, qui sont vraiment très à risque?

[*Traduction*]

**M. Bradley :** C'est une excellente question, et on la pose souvent au secteur. Comme vous le signalez, il existe une différence importante entre la taille de la plus grande de nos entreprises et la plus petite. Nous nous concentrons — tout comme la North American Electric Reliability Corporation — généralement sur ces entreprises qui font partie du réseau de production-transport. Il s'agit de toute entreprise qui est interconnectée à un niveau de transmission où les conséquences d'une atteinte à la sécurité pourraient avoir un effet de cascade.

Nous travaillons avec nos plus petits membres afin de les aider avec tout ce qui va de la cyberhygiène aux pratiques exemplaires et à l'échange de renseignements. Mais l'effort de l'association et de l'Amérique du Nord dans ce domaine a toujours visé principalement à s'assurer que tout le monde qui fait partie du réseau de production-transport d'électricité en Amérique du Nord jouit d'un niveau de sécurité plus que suffisant.

Depuis un certain nombre d'années, notre préoccupation, bien avant que la loi ne soit rédigée — et je fais partie de ces discussions depuis près de 20 ans pour ce qui est des cadres législatifs — a toujours été d'avoir un secteur d'électricité assez mature pour ce qui est de son approche, mais ma plus grande inquiétude tient à toutes les interdépendances. Elle ne concerne pas nécessairement mes plus petits membres; ce sont surtout les autres secteurs dont nous dépendons, qu'il s'agisse des télécommunications, de la finance, de l'eau ou du transport.

While we have very robust cybersecurity standards that the sector must maintain, we are looking at this legislation to be able to set a bar for all of the sectors, including those sectors we depend upon as well.

**Senator Boehm:** Thank you, witnesses, for being with us. My questions are related to our labour representatives here.

Obviously, workers and unionized workers are the ones who are at the forefront of implementing cybersecurity policies. Do you have concerns about training and how that will fit in, assuming the bill is passed and implemented?

**Mr. Leclerc:** Absolutely. Thank you for the question.

The company I work for, which shall remain nameless, refuses to allocate budgets to train people onshore because they'd rather package off the staff here in Canada and hire in India or the Philippines at pennies on the dollar. So it is a huge concern.

**Senator Boehm:** How are you addressing it? Are you speaking with management regularly about this? Are you looking at examples from other countries?

**Mr. Leclerc:** Absolutely. We try to negotiate in the collective bargaining process to have budgets allocated toward training and maintaining certifications for different equipment and hardware. Some clients use Cisco, some use Avaya and some use Fujitsu. You have technicians and programmers who are certified to work on that equipment, and they need to maintain certifications just to stay employable.

When you're dealing with an employer that refuses to allocate the funds to train people to maintain their certifications, you're creating vulnerabilities for your client base. You're not investing in your workforce. That's a huge concern.

**Senator Boehm:** Are you in touch with other labour representatives in other countries about this?

**Mr. Leclerc:** Absolutely.

Not in other countries but here in Canada.

**Senator Boehm:** And everyone has a similar concern?

**Mr. Leclerc:** We all have similar concerns.

Bien que nous disposions de normes de cybersécurité très robustes que le secteur doit maintenir, nous aimerions que cette loi puisse déterminer un seuil pour tous les secteurs, y compris ceux dont nous dépendons également.

**Le sénateur Boehm :** Merci, chers témoins, d'être avec nous. Mes questions concernent nos représentants syndicaux ici présents.

Évidemment, les travailleurs et les travailleurs syndiqués sont ceux qui sont à l'avant-plan de la mise en œuvre des politiques de cybersécurité. Avez-vous des inquiétudes liées à la formation et à la façon dont cela sera intégré, en présumant que le projet de loi soit adopté et mis en œuvre?

**M. Leclerc :** Absolument. Je vous remercie de poser la question.

L'entreprise pour laquelle je travaille, que je ne nommerai pas, refuse d'affecter des budgets pour former du personnel ici sur place parce qu'elle préfère licencier le personnel ici au Canada et embaucher des employés en Inde ou aux Philippines, à un prix dérisoire. Il s'agit donc d'une grande préoccupation.

**Le sénateur Boehm :** Comment y remédiez-vous? Vous entretenez-vous souvent avec la direction à ce sujet? Examinez-vous des exemples d'autres pays?

**M. Leclerc :** Absolument. Nous essayons de négocier dans le processus de convention collective afin que des budgets soient affectés à la formation et au maintien des certifications pour différents équipements et logiciels. Certains clients utilisent Cisco, d'autres Avaya, et d'autres, Fujitsu. Des techniciens et des programmeurs ont la certification requise pour travailler avec ces équipements, et ils doivent maintenir les certifications juste pour rester employables.

Lorsque vous avez affaire à un employé qui refuse d'affecter des fonds pour former le personnel afin qu'il maintienne ses certifications, vous créez des vulnérabilités pour votre clientèle. Vous n'investissez pas dans votre main-d'œuvre. C'est une énorme préoccupation.

**Le sénateur Boehm :** Communiquez-vous avec d'autres représentants syndicaux d'autres pays à ce sujet?

**M. Leclerc :** Absolument.

Pas dans d'autres pays, mais ici, au Canada.

**Le sénateur Boehm :** Est-ce que tout le monde a une préoccupation semblable?

**M. Leclerc :** Nous avons tous des préoccupations semblables.

[*Translation*]

**Nathalie Blais, Research Representative, Canadian Union of Public Employees:** I'd like to add that something we're seeing more often is that unionized employees are being kept away from what would be considered the technical core. Subcontractors in other countries have access to our telecommunications networks while our employees do not. That's a concern. It creates an additional entry point into the networks.

**Senator Boehm:** Thank you very much.

[*English*]

Mr. Bradley, do you have a comment on this issue?

**Mr. Bradley:** Training is certainly critical. We're not facing the same kind of challenge with respect to the offshoring of our core activities. There is a clear delineation in the electricity sector between information technologies and operating technologies. Operating technologies are not offshored or sent elsewhere.

**Senator Boehm:** Are you in touch with other countries and jurisdictions in terms of how there would be an application?

**Mr. Bradley:** Absolutely. We are very active on the North American basis through a variety of means, such as the North American Electric Reliability Corporation, but we also have an international electricity summit. That is literally across the globe. It tends to be at the CEO level, but it's also an opportunity at those meetings to have these kinds of conversations because the challenges are the same, regardless of where you happen to be, whether you're in the United States, Japan, Australia, the U.K. or Canada.

**Senator Boehm:** Thank you very much.

[*Translation*]

**Senator Carignan:** I'm trying to understand how an external call centre works. I'm trying to get a sense of the risks. From what I understand of the system, data centres must be located in Canada. When people call, they communicate with external staff who have limited access in order to provide service. If I call Videotron, I'm calling Chicoutimi — I recognize the accent — but if I call Bell, I know I've reached someone in some part of Morocco. There hasn't been an incident. At least, we haven't heard about any incidents. Is this a real risk? It would be terrible for companies if it happened. I imagine they're all taking this very seriously and making sure they minimize the risk. Unless you have whistle-blowers, like the Canada Revenue Agency?

[*Français*]

**Nathalie Blais, conseillère à la recherche, Syndicat canadien de la fonction publique :** Si je peux me permettre, nous voyons de plus en plus que les employés syndiqués sont tenus loin de ce qui est considéré comme le noyau technique. Il y a des sous-traitants dans d'autres pays qui ont accès à nos réseaux de télécommunication, alors que nos employés n'y ont plus accès. C'est une préoccupation. Cela crée une porte d'entrée supplémentaire dans les réseaux.

**Le sénateur Boehm :** Merci beaucoup.

[*Traduction*]

Monsieur Bradley, avez-vous quelque chose à dire à ce sujet?

**M. Bradley :** Il est certain que la formation est essentielle. Nous ne sommes pas exposés au même type de défi pour ce qui est de la délocalisation de nos activités principales. Il y a une délimitation claire dans le secteur de l'électricité entre les technologies de l'information et les technologies d'exploitation. Les technologies d'exploitation ne sont pas délocalisées ou envoyées ailleurs.

**Le sénateur Boehm :** Communiquez-vous avec d'autres pays et administrations pour savoir comment on pourrait les appliquer?

**M. Bradley :** Absolument. Nous sommes très actifs en Amérique du Nord, et nous utilisons divers moyens, comme la North American Electric Reliability Corporation, mais nous avons également un sommet international sur l'électricité. Il se tient littéralement partout dans le monde. Il réunit habituellement des PDG, mais ces réunions sont aussi l'occasion d'avoir ces types de conversations, parce que les défis sont les mêmes, peu importe l'endroit où vous vous trouvez, que ce soit les États-Unis, le Japon, l'Australie, le Royaume-Uni ou le Canada.

**Le sénateur Boehm :** Merci beaucoup.

[*Français*]

**Le sénateur Carignan :** J'essaie de comprendre comment fonctionne un système de centre d'appels externe. J'essaie de voir quels sont les risques. Selon ce que je comprends du système, les centres de données doivent être détenus au Canada. Quand on appelle, on entre en contact avec du personnel externe qui a des accès limités pour donner le service. Si j'appelle Vidéotron, j'appelle à Chicoutimi — je reconnais l'accent —, mais si j'appelle Bell, je sais que je suis quelque part au Maroc. On n'a pas eu d'incident. En tout cas, on n'a pas entendu parler d'incident qui se serait produit. Est-ce un risque réel? Ce serait terrible pour ces entreprises que cela se produise. J'imagine qu'elles sont sérieuses dans ce qu'elles font et qu'elles s'assurent de limiter les risques. À moins que vous ayez des lanceurs d'alerte, comme à l'Agence du revenu du Canada?

**Mr. Leclerc:** Thank you for the question. There are examples of Videotron outsourcing to Egypt. At one point, there was a mutiny because the value of the Egyptian currency plummeted. Workers in North African countries ended up working for nothing, basically. That creates a risk when a worker is starving and can't pay the rent—

**Senator Carignan:** I can see the risk of someone getting mad and taking drastic action.

**Mr. Leclerc:** Not just taking drastic action, but downloading a customer's data onto a USB key and taking off with it.

**Senator Carignan:** Can someone do that, technically?

**Mr. Leclerc:** Absolutely. Look at what happened at Desjardins not that long ago.

**Senator Carignan:** Yes, but they can't do it anymore. It was an issue at Desjardins, but they put security keys in place to prevent it from happening again.

**Mr. Leclerc:** Yes, but—

**Senator Carignan:** I imagine they have security keys over there, too. I'm playing devil's advocate. I'm trying to understand your concern.

**Ms. Blais:** I think the main risk is associated with providing our information over the phone. If I call Videotron, I end up in Egypt and they ask me questions. What is my mother's maiden name, my driver's licence number and so on? I myself was a victim of partial identity theft involving a telecommunications company. Debt collectors contacted me at home. What saved the day and saved me from having to pay was that not quite all the information was correct. Because of that incorrect information, I was able to prove to the company that I was not the one who had made those purchases with the vendor.

I was off the hook, but when I give that information over the phone and it leaves the country, there's nothing preventing someone from taking notes for a period of time and getting that information. I understand what you're trying to say. Yes, companies have security measures. It's not perfect in Canada, but at least in Canada it stays in Canada and I have recourse against the company. When that information leaves the country, I have recourse against the company, which has a contract with a subcontractor. I don't know what's in that contract. Does it protect personal information?

**Senator Carignan:** When it comes to protecting personal information, I do have recourse against a Canadian company in Canada, regardless of where the security breach happened.

**M. Leclerc :** Merci pour la question. On a des exemples de l'impartition que Vidéotron fait en Égypte. À un moment donné, il y a eu une mutinerie, car il y a eu une chute de la devise égyptienne. Cela a fait en sorte que les employés de pays nord-africains se retrouvaient à travailler pour rien, dans le fond. Cela crée un risque quand un travailleur est affamé et ne peut pas payer son loyer...

**Le sénateur Carignan :** Je comprends le risque qu'il puisse se fâcher et mettre le feu.

**M. Leclerc :** Pas seulement mettre le feu, mais télécharger les données d'un client sur une clé USB et partir avec.

**Le sénateur Carignan :** Est-ce qu'il peut le faire, techniquement?

**M. Leclerc :** Absolument. Regardez ce qui s'est passé chez Desjardins il n'y a pas si longtemps.

**Le sénateur Carignan :** Oui, mais ils ne peuvent plus le faire. Chez Desjardins, c'était un enjeu, mais ils ont mis des clés pour empêcher que cela se reproduise.

**M. Leclerc :** Oui, mais...

**Le sénateur Carignan :** J'imagine qu'ils ont des clés là-bas aussi. Je me fais l'avocat du diable. J'essaie de comprendre votre préoccupation.

**Mme Blais :** Je pense que le risque principal, c'est de donner nos informations au téléphone. J'appelle Vidéotron et j'arrive en Égypte. Qu'est-ce qu'on me demande? Le nom de jeune fille de ma mère, le numéro de mon permis de conduire ou autre chose. Personnellement, j'ai été victime d'un vol d'identité partiel. C'était avec une compagnie de télécommunication. Des firmes de recouvrement m'ont contactée chez moi. Ce qui m'a permis de sauver la face et de ne pas avoir à payer, c'est que toutes les informations étaient correctes, sauf quelques-unes. Ces dernières m'ont permis de prouver à la compagnie que ce n'était pas moi qui avais engagé les frais auprès du fournisseur.

J'ai donc été dégagée, mais lorsque je donne ces informations au téléphone et qu'elles sortent complètement du pays, il n'y a rien qui empêche quelqu'un de prendre des notes pendant un certain temps et d'avoir ces informations. Je comprends ce que vous voulez dire. Oui, les compagnies mettent en place des mesures de sécurité. Ce n'est pas sans failles au Canada, mais au moins, au Canada, cela reste au Canada et j'ai un recours contre la compagnie. À partir du moment où c'est à l'extérieur du pays, j'ai un recours contre la compagnie qui, elle, a un contrat avec le sous-traitant. Je ne sais pas ce qu'il y a dans le contrat. Est-ce que cela protège les informations personnelles?

**Le sénateur Carignan :** Du point de vue de la protection des renseignements personnels, j'ai quand même un recours contre une compagnie canadienne au Canada, peu importe l'origine de la fuite.

**Ms. Blais:** Yes, but once the privacy genie is out of the bottle, it rarely goes back in again. Once things get out in other countries, it's even worse.

**Senator Carignan:** I understand, but I'm more concerned about aspects related to electricity, which could fall prey to cyberattacks that crash the system. I'm not underestimating the importance of breaches that affect individuals, but do they have tools or access to technical information that could enable them to crash the system or demand a ransom, kind of like the essential nature of electricity?

**Mr. Leclerc:** The answer is yes, and it happens on a daily basis. Our union office was the victim of a ransomware attack less than a year ago.

**Ms. Blais:** The other thing you need to know is that, when technical jobs, such as design jobs in Algeria and India, are subcontracted, people abroad have access to our telecom system plans.

**Senator Carignan:** CAE has engineers in India, and it's no less secure for airplanes. I'm trying to be objective about your risk.

**Ms. Blais:** I can't comment further on that because that's beyond my technical skills, but my understanding is that there really is information in Egypt, where the subcontracting company is owned by the Egyptian government, which is an authoritarian government and not necessarily a friend to Canada. I don't know if they have the technical means to get their hands on that information or not.

[*English*]

**Senator Cardozo:** My question is for Mr. Hatfield.

You have raised the issue of trust in the system, which is really important. The purpose of this bill is to secure the Canadian telecommunications system against a range of threats. My question to you is: Does it do it in some ways, and is it your feeling that it's overkill and that it allows the government to gather too much information about people?

**Mr. Hatfield:** I want to be quite specific about what we're asking for here, because we heard in the last panel that people are saying there needs to be some broadness so the bill can be flexible to different technologies as they emerge.

We agree with that. We're not asking for the bill to be made incredibly specific and narrow across the board. What we want to do is make sure that as the bill evolves — as it is in place for decades, potentially — there are some clear guiding principles

**Mme Blais :** Oui, mais une fois le génie sorti de la bouteille en matière de vie privée, c'est très rare qu'il y entre à nouveau. Une fois sorti à l'étranger, c'est encore pire.

**Le sénateur Carignan :** Je comprends, mais je suis plus inquiet pour des éléments liés à l'électricité où il pourrait se produire des cyberattaques et où on peut faire planter le système. Je ne sous-estime pas l'importance des fuites qui touchent les individus, mais est-ce qu'ils ont des outils ou un accès à de l'information technique qui pourrait leur permettre de faire planter le système ou de demander des rançons, un peu comme l'aspect essentiel de l'électricité?

**M. Leclerc :** La réponse est oui, et ça se produit tous les jours. Notre bureau syndical a été victime d'un rançongiciel il n'y a pas tout à fait un an.

**Mme Blais :** Ce que vous devez savoir aussi, c'est dans le cas des emplois techniques qui sont sous-traités, par exemple ceux de dessin de plan en Algérie ou en Inde, les gens qui sont à l'étranger ont accès aux plans des systèmes de télécommunication ici.

**Le sénateur Carignan :** La CAE aussi prend des ingénieurs en Inde et ce n'est pas moins sécuritaire pour les avions. J'essaie d'objectiver votre risque.

**Mme Blais :** Je ne peux pas aller plus loin, mes compétences techniques ne vont pas plus loin, mais selon ce que je comprends, il y a vraiment des informations en Égypte où la compagnie de sous-traitance est la propriété du gouvernement égyptien, qui est un gouvernement autoritaire et qui n'est pas nécessairement un de nos amis. Je ne sais pas s'ils ont des moyens techniques pour mettre la main sur cette information ou non.

[*Traduction*]

**Le sénateur Cardozo :** Ma question s'adresse à M. Hatfield.

Vous avez évoqué la question de la confiance dans le système, qui est très importante. L'objectif du projet de loi est de protéger le système canadien de télécommunications contre un éventail de menaces. Ma question pour vous est la suivante : arrive-t-il à le faire de certaines manières, et pensez-vous qu'il est exagéré et qu'il permet au gouvernement de recueillir trop d'information sur les gens?

**M. Hatfield :** Je tiens à préciser ce que nous demandons ici, car nous avons entendu des gens dire dans le dernier groupe de témoins qu'il doit y avoir une certaine ouverture pour que le projet de loi s'adapte aux différentes technologies à mesure qu'elles apparaissent.

Nous y sommes favorables. Nous ne demandons pas de préciser ou de limiter de façon générale le projet de loi. Ce que nous voulons, c'est nous assurer que, à mesure que le projet de loi évolue — puisqu'il sera en place pour des dizaines d'années,

and limits on it. Things like an indefinite secret order architecture, where they can make a secret order and then, well, gosh, you can't talk about the secret order, so we need another secret order to build on that, and over a few decades, you can wind up with a whole system of governance set up, none of which is visible to the Canadian public.

That's a huge concern for us here. We want to see the bill done, but we want to see a few more safeguards put in place to both protect us from that secrecy and also ensure that our data is treated appropriately.

**Senator Cardozo:** I haven't thought this through completely, but there are other acts where certain warrants are issued by the RCMP, for example, with the approval of a judge, even though that takes place in secret. Would something like this be of assurance to you?

**Mr. Hatfield:** I think that's helpful when it's appropriate. The push back that we've had on that is that sometimes we have to act quickly and something must be done immediately. What we're trying to allow for is that, yes, sometimes something has to be done immediately, and the minister, perhaps, makes an urgent secret order, but at some phase, there is some kind of public accounting for what's happened. There is some report where they say, "We had to do this," but a month or six months later — whenever it is — they come back and say, "This thing happened, and this is what we can tell you about it." There is some transparency to the system.

**Senator Cardozo:** Thank you.

A quick question to Mr. Leclerc. Mr. Bradley talked about some types of information such as the internal administration of an electricity company, that this information is not available to foreign workers — I think maybe some of the things around billing. Maybe I'm paraphrasing it wrong, but is the information you're talking about divisible in terms of what foreign workers would see and what they would not see?

**Mr. Leclerc:** Thank you for the question. The foreign workers have access to not just your billing information, but now they have our accounts payable, they have our payroll and they have dispatching capabilities.

As time goes on, the companies become more inclined to outsource and offshore more and more tasks to save more money. It's just a matter of corporate greed.

**Senator Cardozo:** But the operation of the telecom, do the people who work on that, are they strictly on Canadian soil?

peut-être —, il soit régi par des limites et des principes directeurs clairs. Des choses comme une architecture de décrets secrets indéfinis, où l'on peut faire un décret secret puis, et bien, vous ne pouvez pas en parler, alors il nous faut un autre décret secret pour nous appuyer là-dessus, et dans quelques décennies, vous vous retrouvez avec tout un système de gouvernance mis sur pied, dont rien n'est visible au public canadien...

C'est une énorme préoccupation pour nous. Nous voulons voir le projet de loi se concrétiser, mais qu'un plus grand nombre de mesures de protection soient mises en place pour nous protéger contre ce secret et nous assurer que nos données sont traitées de manière appropriée.

**Le sénateur Cardozo :** Je n'ai pas réfléchi entièrement à la question, mais il y a d'autres lois où certains mandats sont délivrés par la GRC, par exemple, avec l'approbation d'un juge, même si cela se fait en secret. Est-ce quelque chose qui vous rassurerait?

**M. Hatfield :** Je pense que c'est utile lorsque c'est approprié de le faire. Nous avons essuyé de la résistance, parce que nous devons parfois agir rapidement et faire quelque chose immédiatement. Ce que nous essayons d'autoriser, c'est que, oui, il faut parfois agir immédiatement, et peut-être que le ministre doit prendre un décret secret urgent, mais à un certain stade, il faut rendre compte au public de ce qui est arrivé. Il faut produire un rapport qui dit : « Nous avons dû faire ceci », mais un mois ou six mois plus tard — peu importe quand — il revient dire : « Cette chose est arrivée, et voici ce que nous pouvons faire à ce sujet. » Il y a une certaine transparence dans le système.

**Le sénateur Cardozo :** Merci.

J'ai une brève question à poser à M. Leclerc. M. Bradley a parlé de certains types de renseignements, comme ceux relatifs à l'administration interne d'une entreprise d'électricité, qui ne sont pas accessibles aux travailleurs étrangers — je pense que c'est peut-être le cas pour certaines choses liées à la facturation. Je paraphrase peut-être mal, mais les renseignements dont vous parlez sont-ils fragmentables, c'est-à-dire les éléments d'information que les travailleurs étrangers verraient et ceux qu'ils ne verraient pas?

**M. Leclerc :** Merci de la question. Les travailleurs étrangers n'ont pas accès seulement à vos renseignements sur la facturation; ils ont maintenant accès à nos comptes créditeurs, à notre paye, et ils ont des capacités de distribution.

Au fil du temps, les entreprises ont davantage tendance à sous-traiter et à délocaliser de plus en plus de tâches pour économiser davantage d'argent. C'est simplement une question de cupidité des entreprises.

**Le sénateur Cardozo :** Mais les gens qui travaillent dans le domaine des télécommunications sont-ils strictement en sol canadien?

**Mr. Leclerc:** No. I said it in my introduction that design engineers to programmers — programming network infrastructure is done in India more and more.

There is a certain percentage of the clientele that stays onshore. If you're a Fortune 500 company, for example, or different levels of government, that stays onshore, but if you're not fortunate enough to be on that list of customers that has to be processed onshore, good luck.

**Senator Kutcher:** Thank you to our witnesses.

My question is to our labour representatives. Thank you for raising the concern of offshoring work with the telecoms.

Recently, Canada's three largest telecoms — Telus, Bell and Rogers — have moved into the health care space big time. In the past, my understanding was that we had remote reporting of diagnostic imaging, which was concerning enough, but now some of the telecoms will actually provide direct health care services, and other telecoms will provide the infrastructural and communications support for independent private service health care providers.

The provinces don't capture that data. It's not in provincial databases. It's a private company providing the services, and these services are provided across all provinces, not just within one province.

As far as I know, the federal government — I could be wrong — doesn't have jurisdiction in this particular part. This seems like a bit of a grey area, and if some of the work offshoring of diagnostic work or therapeutic work occurs outside of the country, can this bill address any of those things? Should it address those things? How can we address those things?

**Mr. Leclerc:** Personally, I can't speak to this because these companies work in silos. Your telecom business is under federal jurisdiction; it's one silo. The health care side of the house, telemedicine and other products and services in that realm, that's another silo, and they don't communicate very well.

Obviously, they exchange services with each other, because the telecom business provides data connectivity to the health care side of the house, but are there risks? Absolutely.

[*Translation*]

**Ms. Blais:** I'll add that there is another reason to worry. Technological advances such as 5G for cellphones combined with artificial intelligence with its scanners and sensors have led to self-driving cars and the internet of things. Now we're talking

**M. Leclerc :** Non. J'ai dit dans ma déclaration liminaire que, des ingénieurs en conception aux programmeurs, la programmation des infrastructures de réseau se fait de plus en plus en Inde.

Un certain pourcentage de la clientèle reste sur place. Si vous êtes une entreprise Fortune 500, par exemple, ou un autre ordre de gouvernement, cette clientèle reste sur place, mais si vous n'avez pas la chance de figurer sur la liste des clients qui doivent être traités sur place, bonne chance.

**Le sénateur Kutcher :** Merci à nos témoins.

Ma question s'adresse à nos représentants syndicaux. Merci d'avoir soulevé la préoccupation de la délocalisation du travail dans le secteur des télécommunications.

Récemment, les trois plus grandes entreprises de télécommunications du Canada — Telus, Bell et Rogers — se sont lancées à fond dans le secteur des soins de santé. Par le passé, je croyais que nous avions des rapports à distance de l'imagerie diagnostique, ce qui était déjà assez inquiétant, mais maintenant, certaines entreprises de télécommunication fourniront des services de soins de santé directs, et d'autres fourniront le soutien en matière d'infrastructure et de communication aux fournisseurs de soins de santé privés indépendants.

Les provinces ne saisissent pas ces données. Cela ne figure pas dans les bases de données provinciales. C'est une entreprise privée qui fournit ces services, et ceux-ci sont offerts dans toutes les provinces, et non pas seulement dans une seule province.

À ma connaissance, le gouvernement fédéral — je peux me tromper — n'a pas compétence dans ce domaine particulier. Cela semble être une zone grise, et si une partie du travail de diagnostic ou de traitement est délocalisée à l'extérieur du pays, ce projet de loi peut-il régler ces problèmes? Devrait-il régler ces problèmes? Comment pouvons-nous régler ces problèmes?

**M. Leclerc :** Personnellement, je ne peux pas me prononcer à cet égard, car ces entreprises travaillent en vase clos. Votre entreprise de télécommunications relève de la compétence fédérale; c'est un vase clos. Le secteur des soins de santé, la télémédecine et d'autres produits et services dans ce domaine, c'est un autre vase clos, et ils ne communiquent pas très bien.

Évidemment, ils échangent des services entre eux, car l'entreprise de télécommunications fournit une connectivité de données au secteur des soins de santé, mais y a-t-il des risques? Absolument.

[*Français*]

**Mme Blais :** J'ajoute qu'il y a une autre raison de s'inquiéter. Avec l'évolution technologique, comme en téléphonie cellulaire, avec la 5G combinée à l'intelligence artificielle, avec les détecteurs et les capteurs, on s'en va vers des véhicules

about remote operations. This is all the more reason to make sure that Canadian telecom networks are truly secure in Canada. There is also the whole data protection aspect, which is covered by federal law because telecoms are federally regulated businesses.

The fact remains that there are gaps. Your data could end up overseas. If my driver's licence number ends up in Egypt, I have no control over what happens afterward. In 2020, we launched a public awareness campaign about the situation and conducted a survey. Four out of five Quebecers were very worried when we told them their personal information was processed offshore. That was something really important to them.

[*English*]

**Senator Batters:** My question is to Mr. Hatfield from OpenMedia. At the House of Commons committee on Bill C-26, you stated this in your testimony:

> . . . privacy rights must be entrenched. Personal information must be clearly defined as confidential and forbidden from being shared with foreign states, which are not subject to Bill C-26's checks and balances.

I know Canadians will find this to be very alarming. You noted it in your opening remarks today, but please tell us more about how that schism in Bill C-26 could be fixed?

**Mr. Hatfield:** Yes. One of the most important remaining issues here is that there is a very high chance that some personal information is it going to be caught up in the operation of Bill C-26. It's going to enter the hands of Canadian law enforcement agencies, which are doing appropriate work relating to cybersecurity, but currently there is no safeguard to make sure they don't use that information for other purposes and may even end up sharing it with some of our Five Eyes intelligence partners, who can do whatever they want with that data.

Many of them have intelligence acts that don't apply to noncitizens, so once that data is out of Canadian hands, it's open season. We don't want to see that happening under Bill C-26. That's very alarming, especially knowing that the world is changing, democracy is under threat and some governments are doing more invasive things to their citizens. We worry about data originally collected for appropriate purposes by the Canadian government eventually being misused against Canadians.

automatisés, vers l'Internet des objets, et on parle de pouvoir faire des opérations à distance. Ce sont là des raisons de plus de s'assurer que les réseaux de télécommunication sont vraiment sécuritaires au Canada. De plus, il y a tout l'aspect de la protection des données qui est couvert par la loi fédérale, puisque les entreprises de télécommunication sont des entreprises fédérales.

N'empêche, il y a tout de même certaines failles; si vos données se retrouvent à l'étranger, si mon numéro de permis de conduire est rendu en Égypte, je n'ai pas de contrôle sur ce qui arrivera par la suite. En 2020, on avait commencé une campagne pour alerter le public sur cette situation et on avait fait faire un sondage : quatre Québécois sur cinq étaient très inquiets quand on leur disait que leurs informations personnelles étaient traitées à l'étranger. C'est vraiment quelque chose d'important pour les gens.

[*Traduction*]

**La sénatrice Batters :** Ma question s'adresse à M. Hatfield d'OpenMedia. Vous avez déclaré ceci dans votre témoignage devant le comité de la Chambre des communes concernant le projet de loi C-26 :

> […] les droits à la vie privée doivent être garantis. Les renseignements personnels doivent être clairement définis comme étant confidentiels, et il doit être interdit de les communiquer à des États étrangers, qui ne sont pas assujettis aux freins et contrepoids prévus dans le projet de loi C-26.

Je sais que les Canadiens trouveront cela très alarmant. Vous l'avez souligné dans votre déclaration liminaire aujourd'hui, mais pouvez-vous nous en dire plus sur la façon dont on pourrait corriger ce schisme dans le projet de loi C-26?

**M. Hatfield :** Oui. L'un des problèmes les plus importants qui subsistent ici est qu'il y a de très fortes probabilités que certains renseignements personnels soient touchés par l'application du projet de loi C-26. Ils tomberont entre les mains d'organismes canadiens d'application de la loi, qui font un travail approprié en matière de cybersécurité, mais il n'existe actuellement aucune mesure de protection pour que l'on puisse s'assurer qu'ils n'utilisent pas ces renseignements à d'autres fins et qu'ils peuvent même finir par les partager avec certains de nos partenaires en matière de renseignement du Groupe des cinq, qui peuvent faire ce qu'ils veulent avec ces données.

Beaucoup d'entre eux ont des lois sur le renseignement qui ne s'appliquent pas aux non-citoyens, donc une fois que ces données ne sont plus entre les mains des Canadiens, le champ est libre. Nous ne voulons pas que cela se produise dans le cadre du projet de loi C-26. C'est très alarmant, surtout quand on sait que le monde change, que la démocratie est menacée et que certains gouvernements se montrent plus intrusifs envers leurs citoyens. Nous craignons que les données initialement recueillies à des

**Senator Batters:** Thanks for setting those out as time bombs of this bill, because I agree that there are some very concerning things. You also said at the House of Commons committee:

> . . . when the use of those powers is challenged in court, there must be no secret evidence. Special advocates should be appointed to ensure all evidence is duly tested.

Can you tell us more about that, and how you propose to amend Bill C-26 to fix that?

**Mr. Hatfield:** It's a huge issue, and we would still like to see Bill C-26 include that special advocate. People have referred to the situation regarding TikTok that we have right now. I can't tell you what's going on there. The government won't tell us. They're saying, "There is a big problem with TikTok. We had to do something and we've done it." Was it a well-founded reason or not? I don't know, and there is no special advocate in that system to say, "This person looked at it, and it was appropriate." Under Bill C-26, we have no person to perform that kind of judgment currently.

**Senator Batters:** Speaking about this is something akin to the Office of the Intelligence Commissioner like with other types of national security-related cases, right?

**Mr. Hatfield:** Yes, special advocates exist in several other cases and serve a useful function there.

**Senator LaBoucane-Benson:** My question is also for Mr. Hatfield. The Civil Society brief that you signed onto — thank you for submitting that; it's in-depth and very interesting — says that Bill C-26 allows the government to disclose confidential information "to anyone." That's on page 11. The concerns you have raised are definitely legitimate. I just want to ensure we're not engaging in hyperbole. Under the Privacy Act, government institutions may only use personal information for the purpose for which it was collected. Do you agree that Bill C-26 — like all acts of Parliament — will be subject to the Privacy Act's requirements?

**Mr. Hatfield:** Certainly subject, but information can be passed from some hands to others nominally for cybersecurity purposes, which in effect are actually used for a much broader

fins appropriées par le gouvernement canadien ne soient éventuellement utilisées à mauvais escient contre les Canadiens.

**La sénatrice Batters :** Merci d'avoir qualifié ces éléments de bombes à retardement de ce projet de loi, car je reconnais que celui-ci contient des éléments très préoccupants. Vous avez également déclaré devant le comité de la Chambre des communes :

> […] lorsque l'utilisation de ces pouvoirs sera contestée devant les tribunaux, aucune preuve secrète ne devra être autorisée. Des avocats spéciaux devraient être nommés pour évaluer toutes les preuves rigoureusement.

Pouvez-vous nous en dire plus à ce sujet et nous dire comment vous proposez de modifier le projet de loi C-26 pour régler ce problème?

**M. Hatfield :** C'est un énorme problème, et nous aimerions quand même que le projet de loi C-26 inclue un avocat spécial. Certains ont évoqué la situation actuelle concernant TikTok. Je ne peux pas vous dire ce qui se passe dans ce cas. Le gouvernement ne veut pas nous le dire. Il dit : « Il y a un gros problème avec TikTok. Nous devions faire quelque chose, et nous l'avons fait. » Était-ce une raison justifiée ou non? Je ne sais pas, et il n'y a pas d'avocat spécial dans ce système pour dire : « Cette personne a examiné la question, et c'était approprié. » En vertu du projet de loi C-26, nous n'avons personne pour rendre ce genre de jugement actuellement.

**La sénatrice Batters :** Le fait d'en parler, c'est un peu comme le Bureau du commissaire au renseignement, comme dans d'autres types d'affaires liées à la sécurité nationale, n'est-ce pas?

**M. Hatfield :** Oui, il existe des avocats spéciaux dans plusieurs autres affaires, et ils jouent un rôle utile à cet égard.

**La sénatrice LaBoucane-Benson :** Ma question s'adresse également à M. Hatfield. Le mémoire des groupes de la société civile auquel vous avez souscrit — merci de l'avoir soumis, il est approfondi et très intéressant — indique que le projet de loi C-26 permet au gouvernement de divulguer des renseignements confidentiels « à quiconque ». C'est à la page 11. Les préoccupations que vous avez soulevées sont tout à fait légitimes. Je veux simplement m'assurer que nous ne nous livrons pas à des exagérations. En vertu de la Loi sur la protection des renseignements personnels, les institutions gouvernementales ne peuvent utiliser les renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis. Êtes-vous d'accord pour dire que le projet de loi C-26 — comme toutes les lois du Parlement — sera assujetti aux exigences de la Loi sur la protection des renseignements personnels?

**M. Hatfield :** Certainement, mais des renseignements peuvent être transmis de certaines mains à d'autres, censément à des fins de cybersécurité; en réalité, ils sont utilisés à des fins beaucoup

set of purposes, particularly if the data is eventually handed outside of Canada. There is no application of the Privacy Act whatsoever in that case.

**Senator M. Deacon:** Thank you all for joining us today. My first question is for Mr. Bradley. You may have heard me touch on this in the first round with Bruce Power. It concerns international cooperation. Our power grids cross borders, and I want to get a sense from you about how our American partners view us when it comes to keeping our grids safe from cyberattacks and what they think of this legislation. Will it do much to build trust in our ability to protect ourselves in a North American grid?

**Mr. Bradley:** Thank you. That's an excellent question. Of course, it is top of mind for us, and it has been for the last couple of weeks as to whether or not the political changes taking place in the United States will have any impact on us.

However, we are in a sector, where for more than 100 years, our systems have been tightly and closely integrated. We have a North American approach to security and cybersecurity, but we've had a regime for critical infrastructure protection cyber-standards through the North American Electric Reliability Corporation, now for close to 20 years. So it is now kind of in the DNA of the sector to operate and to think about this from a North American standpoint.

That doesn't, however, touch on the potential political risk, and that would be my concern at this stage. From an operating standpoint, we don't anticipate any change in terms of how we work together to ensure the security of the grid. Whether or not there will be political pressure that impacts us, I certainly hope not, but it could be possible.

It's almost like what I was mentioning before about the difference between our information technologies and our operating technologies. The operating technologies are the ones that deal specifically with generating, transmitting and distributing electricity to customers. They are completely separate from the IT technologies. I'm hoping we can keep our operating technologies and how we operate our grids separate from political interference.

**Senator M. Deacon:** Thank you for that. You brought up, through your colleague, safe harbour laws. I'm trying to understand what this would look like in practice better. I was surprised when it came up at earlier committees that a company that warns of imminent or ongoing attack could face litigation for doing so. It seems we want reporting on it after the fact once the damage is done and not being penalized. I wonder what your thoughts are on that.

plus larges, en particulier si les données sont éventuellement transmises à l'extérieur du Canada. La Loi sur la protection des renseignements personnels ne s'applique absolument pas dans ce cas.

**La sénatrice M. Deacon :** Merci à tous d'être parmi nous aujourd'hui. Ma première question s'adresse à M. Bradley. Vous m'avez peut-être entendu traiter de ce sujet lors du premier tour avec Bruce Power. Il s'agit de coopération internationale. Nos réseaux électriques traversent les frontières, et j'aimerais que vous me fassiez part de la façon dont nos partenaires américains nous perçoivent lorsqu'il s'agit de protéger nos réseaux contre les cyberattaques et de ce qu'ils pensent de ce projet de loi. Cela contribuera-t-il à renforcer la confiance dans notre capacité à nous protéger dans un réseau nord-américain?

**M. Bradley :** Merci. C'est une excellente question. Bien sûr, c'est une priorité pour nous, et depuis quelques semaines, nous cherchons à savoir si les changements politiques qui se produisent aux États-Unis auront ou non une incidence sur nous.

Cependant, nous évoluons dans un secteur où, depuis plus de 100 ans, nos systèmes sont étroitement intégrés. Nous avons une approche nord-américaine de la sécurité et de la cybersécurité, mais nous disposons depuis près de 20 ans d'un régime de normes pour assurer la cybersécurité des infrastructures essentielles par l'intermédiaire de la North American Electric Reliability Corporation. Il est donc désormais dans l'ADN du secteur de fonctionner d'un point de vue nord-américain et d'envisager la cybersécurité dans cette même optique.

Cependant, cela n'a rien à voir avec le risque politique potentiel, qui serait ma préoccupation à ce stade. Du point de vue opérationnel, nous ne prévoyons aucun changement dans la manière dont nous travaillons ensemble pour assurer la sécurité du réseau. J'espère que nous ne subirons pas de pression politique, mais cela pourrait être possible.

Cela ressemble presque à ce que je disais tout à l'heure à propos de la différence entre nos technologies de l'information et nos technologies d'exploitation. Les technologies d'exploitation sont celles qui traitent spécifiquement de la production, de la transmission et de la distribution de l'électricité aux clients. Elles sont complètement distinctes des technologies de l'information. J'espère que nous pourrons garder nos technologies d'exploitation et la manière dont nous exploitons nos réseaux à l'abri de toute ingérence politique.

**La sénatrice M. Deacon :** Merci de votre réponse. Vous avez évoqué, par l'intermédiaire de votre collègue, des dispositions ou mesures « d'exonération ». J'essaie de mieux comprendre à quoi cela ressemblerait en pratique. J'ai été étonnée lorsqu'il a été mentionné lors de comités précédents qu'une entreprise qui prévient d'une attaque imminente ou en cours pourrait faire l'objet de poursuites judiciaires pour avoir agi ainsi. Il semble que nous voulions que les signalements soient faits après coup,

**Mr. Bradley:** The sharing of information and the continued sharing of information, which is the background to specifically the issue with respect to safe harbour. If we look at critical information writ large, less than 15% of it is actually owned and operated by the government. Eighty-five per cent of critical infrastructure is industry, so 85% of the information and intelligence about what's happening in cyber-systems is not with the government. It is actually with industry. We've developed good working relationships and information exchanges over the last several years with the CSE and the Cyber Centre, where our information is protected; it is not released. Essentially, we have a virtual safe harbour right now in terms of how our critical information is treated by the Cyber Centre and is treated by the CSE.

We want to make sure that those kinds of protections for critical information will be built into how we implement this legislation. Otherwise, I fear we'll have a chilling effect on that exchange of information and the ability and willingness of critical infrastructure owner operators to share information with the government.

**Senator M. Deacon:** Thank you for that.

**Senator Batters:** Mr. Hatfield, since we have a limited time at this committee, I wanted to give you a bit more time to describe how you would try to fix some of the time bombs you referred to with recommendations contained in that joint submission.

**Mr. Hatfield:** It's about making the bill fit for purpose, and focused on its purpose. We are not in disagreement with the folks who want some version of this bill to happen somewhat quickly, but as you mention the Senate needs to take due time to fill its role of sober second thought and to consider adding a few safeguards.

We would like it to be made very clear that there can be no handover of data gathered under Bill C-26 — certainly not outside of Canada — but ideally not in the regular course of business within the Canadian government as well. There should be cybersecurity information that is used for cybersecurity purposes.

We would also like to see some kind of regime set up that will ensure that, after some period of time, any secret order that's issued to telecoms be disclosed at some level, indicating roughly what's happened so that Canadians can follow the progress of

une fois que les dommages sont causés, sans être pénalisés. Je me demande ce que vous en pensez.

**M. Bradley :** La communication et la communication continue de renseignements : voilà le contexte précis de la question des dispositions ou mesures d'exonération. Si nous examinons les renseignements critiques au sens large, moins de 15 % sont en fait détenus et exploités par le gouvernement. Quatre-vingt-cinq pour cent des infrastructures essentielles sont l'industrie, donc 85 % de l'information et des renseignements sur ce qui se passe dans les cybersystèmes sont non pas entre les mains du gouvernement, mais entre celles de l'industrie. Nous avons établi de bonnes relations de travail et des échanges de renseignements au cours des dernières années avec le CST et le Centre pour la cybersécurité, où nos renseignements sont protégés; ils ne sont pas divulgués. Essentiellement, nous disposons actuellement d'un droit virtuel d'exonération en ce qui concerne la façon dont le Centre pour la cybersécurité et le CST traitent nos renseignements critiques.

Nous voulons nous assurer que ces types de protections des renseignements critiques seront intégrées à la façon dont nous mettrons en œuvre cette loi. Sinon, je crains que nous ayons un effet paralysant sur cet échange de renseignements et sur la capacité et la volonté des propriétaires exploitants d'infrastructures essentielles de partager des renseignements avec le gouvernement.

**La sénatrice M. Deacon :** Merci de cette réponse.

**La sénatrice Batters :** Monsieur Hatfield, comme le temps dont dispose le comité est limité, je voulais vous donner un peu plus de temps pour décrire la façon dont vous tenteriez de désamorcer certaines des bombes à retardement auxquelles vous avez fait référence dans les recommandations contenues dans ce mémoire conjoint.

**M. Hatfield :** Il s'agit de faire en sorte que le projet de loi soit adapté à son objectif et axé sur celui-ci. Nous ne sommes pas en désaccord avec les personnes qui souhaitent qu'une version du projet de loi soit adoptée assez rapidement, mais comme vous le mentionnez, le Sénat doit prendre le temps nécessaire pour remplir son rôle de second examen objectif et envisager d'ajouter quelques mesures de protection.

Nous aimerions qu'il soit bien clair que les données recueillies en vertu du projet de loi C-26 ne peuvent être transmises — certainement pas à l'extérieur du Canada — et idéalement pas dans le cadre des activités normales du gouvernement canadien. L'information en matière de cybersécurité devrait être utilisée à des fins de cybersécurité.

Nous aimerions également qu'un régime soit mis en place pour garantir qu'après un certain temps, toute ordonnance secrète émise à l'égard d'entreprises de télécommunications soit divulguée à un certain niveau, indiquant approximativement ce

Bill C-26 and judge whether it's growing well beyond what it ought to.

**The Chair:** This brings us to the end of our time for this panel. I extend my sincere thanks to Mr. Leclerc, Ms. Blais, Mr. Bradley and Mr. Hatfield.

Thank you for your participation. We appreciate your helpful consideration for this bill.

Our final panel for this evening, I welcome Philippe Dufresne, Privacy Commissioner of Canada from the Office of the Privacy Commissioner of Canada; The Honourable Simon Noël, K.C., Intelligence Commissioner from the Office of the Intelligence Commissioner, it's good to see you again; and Tolga Yalkin, Assistant Superintendent, Regulatory Response Sector, Office of the Superintendent of Financial Institutions. Thank you so much. You each have five minutes and, of course, Mr. Dufresne you're first.

[*Translation*]

**Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada:** Thank you to the chair and members of the committee for this invitation to appear as part of your study of Bill C-26.

Your study is very important because individuals, businesses and all levels of government in Canada remain vulnerable to a range of serious cyber-threats from a variety of cyber-threat actors.

In its *National Cyber Threat Assessment 2025–2026*, which was released in October, the Canadian Centre for Cyber Security underscores "an expanding and complex cyber threat landscape," including a growing risk posed by "state and non-state threat actors" that are targeting Canada's critical infrastructure. The Cyber Centre warns that such incidents could immobilize critical services, disrupt operations, destroy or damage important business data, and reveal sensitive information.

[*English*]

Bill C-26 recognizes that Canada's critical infrastructure must be protected against such threats as they continue to evolve in sophistication and complexity. In addition to potential impacts on the health, safety, security and economic well-being of Canadians, cyber incidents can have significant privacy

qui s'est passé afin que les Canadiens puissent suivre l'évolution du projet de loi C-26 et juger s'il va bien au-delà de ce qu'il devrait faire.

**Le président :** Nous arrivons à la fin de notre séance. Je tiens à remercier sincèrement M. Leclerc, Mme Blais, M. Bradley et M. Hatfield.

Merci de votre participation. Nous vous sommes reconnaissants de l'attention que vous avez accordée à l'étude de ce projet de loi.

Pour notre dernier groupe de témoins de la soirée, je souhaite la bienvenue à Philippe Dufresne, commissaire à la protection de la vie privée du Canada, du Commissariat à la protection de la vie privée du Canada; à l'honorable Simon Noël, c.r., commissaire au renseignement du Bureau du commissaire au renseignement — c'est un plaisir de vous revoir —; et à Tolga Yalkin, surintendant auxiliaire, Secteur des mesures de réglementation, du Bureau du surintendant des institutions financières. Merci beaucoup. Vous avez chacun cinq minutes, et, bien sûr, monsieur Dufresne, vous êtes le premier.

[*Français*]

**Philippe Dufresne, commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada :** Merci beaucoup, monsieur le président et mesdames et messieurs les membres du comité. Je vous remercie de m'avoir invité à comparaître dans le cadre de votre étude sur le projet de loi C-26.

Votre étude est très importante, car les personnes, les entreprises et tous les ordres de gouvernement au Canada demeurent vulnérables à un éventail de cybermenaces graves provenant de divers auteurs.

Dans son *Évaluation des cybermenaces nationales 2025-2026*, publiée en octobre dernier, le Centre canadien pour la cybersécurité fait état d'un « [...] environnement de cybermenaces complexe et en pleine expansion [...] », ainsi que d'un risque croissant posé par des « [...] auteurs de cybermenace étatiques et non étatiques [...] » qui ciblent les infrastructures essentielles du Canada. Le Centre canadien pour la cybersécurité met en garde contre le fait que de tels incidents pourraient paralyser des services essentiels, perturber les opérations, détruire ou endommager des données commerciales importantes et révéler de l'information sensible.

[*Traduction*]

Le projet de loi C-26 reconnaît que les infrastructures essentielles du Canada doivent être protégées contre de telles menaces, puisque celles-ci deviennent de plus en plus perfectionnés et complexes. En plus des répercussions potentielles sur la santé, la sécurité, la sûreté et le bien-être

implications when they result in the unauthorized access to or disclosure of personal information.

Today, the protection of personal information increasingly relies on the security of the digital systems and infrastructure that house and transmit it. Stronger cybersecurity protections can therefore promote privacy interests by reducing the likelihood and impact of data breaches. At the same time, we must ensure that efforts to secure these systems and networks also protect and respect Canadians' fundamental right to privacy.

[*Translation*]

This is not a zero-sum game, and privacy and the public interest are not only compatible — they build on and strengthen one another.

I strongly support the objectives of Bill C-26, and I was pleased to see that several amendments to the bill have been adopted in the spirit of protecting privacy. I was also pleased to see new references to the Privacy Act in the amended text of the bill, which confirms its applicability.

[*English*]

Requiring that any collection, use or disclosure of personal information be both necessary and proportionate is an important privacy principle. While the bill establishes a necessity and reasonableness threshold in certain cases, I would continue to recommend that the committee consider establishing a consistent threshold of necessity and proportionality in Bill C-26 that applies whenever personal information is involved. The adoption of a uniform standard that any collection, use or disclosure of personal information be both necessary in the circumstances to achieve the stated purpose and proportionate to the benefits to be gained would help address potential privacy implications.

In the alternative, should the standard remain unchanged, I would recommend that the committee reintroduce the requirement that information be retained only for as long as necessary. This was added by the SECU committee in the other place but deleted by the House at third reading. Requiring government institutions to conduct privacy impact assessments and to consult my office on new programs or initiatives created under the authorities contained in Bill C-26 would also

économique de la population canadienne, les cyberincidents peuvent avoir des répercussions importantes sur la vie privée lorsqu'ils entraînent l'accès non autorisé à des renseignements personnels ou leur communication.

Aujourd'hui, la protection des renseignements personnels repose de plus en plus sur la sécurité des systèmes et des infrastructures numériques qui les hébergent et les transmettent. Des mesures de protection renforcées en matière de cybersécurité peuvent donc favoriser la protection de la vie privée en réduisant la probabilité et l'incidence des atteintes à la sécurité des données. Parallèlement, nous devons veiller à ce que les efforts déployés pour sécuriser ces systèmes et réseaux protègent et respectent aussi le droit fondamental à la vie privée des Canadiennes et des Canadiens.

[*Français*]

Nous ne sommes pas en présence d'un jeu à somme nulle. La vie privée et l'intérêt public sont non seulement compatibles, mais ils se renforcent mutuellement.

J'appuie fermement les objectifs du projet de loi C-26. J'ai été heureux de constater que de nombreux amendements à ce projet de loi ont été adoptés dans l'esprit de renforcer la protection de la vie privée. J'ai également été heureux de constater que le texte modifié du projet de loi contient de nouvelles références à la Loi sur la protection des renseignements personnels, ce qui confirme son applicabilité dans le domaine.

[*Traduction*]

Le fait d'exiger que la collecte, l'utilisation ou la communication de renseignements personnels soient à la fois nécessaires et proportionnelles est un principe important en matière de protection de la vie privée. Bien que le projet de loi établisse un critère de nécessité et de caractère raisonnable dans certains cas, je continue de recommander que le Comité envisage d'établir dans le projet de loi C-26 un critère uniforme de nécessité et de proportionnalité qui s'appliquerait dans les situations mettant en cause des renseignements personnels. L'adoption d'une norme uniforme selon laquelle la collecte, l'utilisation ou la communication de renseignements personnels doivent être à la fois nécessaires dans les circonstances pour réaliser les fins énoncées et proportionnelles aux avantages procurés contribuerait à tenir compte des conséquences possibles sur la vie privée.

À titre subsidiaire, si la norme reste inchangée, je recommanderais au comité d'envisager de réintroduire l'exigence selon laquelle les renseignements ne seront conservés que le temps nécessaire. Cette exigence avait été ajoutée par le Comité permanent de la sécurité publique et nationale, mais elle a été supprimée par la Chambre des communes à la troisième lecture. Obliger les institutions gouvernementales à réaliser des évaluations des facteurs relatifs à la vie privée et à consulter le

strengthen privacy protections while supporting the public interest and generating trust.

[*Translation*]

Requiring privacy impact assessments, or PIAs — which are currently a policy requirement under the Treasury Board Secretariat's Directive on Privacy Practices, but not a legally binding requirement under privacy legislation — are an important tool for identifying, analyzing and addressing or mitigating privacy issues before initiatives are put in place. PIAs can help to reduce inadvertent harms to privacy as initiatives roll out. That is why I have recommended that the preparation of PIAs should be made a legal obligation for the government under the Privacy Act.

[*English*]

The bill recognizes the importance of collaboration between domestic and international counterparts to ensure that critical infrastructure is protected against a variety of threats. In order to further enhance this collaboration, my office should also be notified about cyber incidents that may result in a material breach. This could include being notified by the Communications Security Establishment Canada whenever it receives a report of a cyber incident that may pose a real risk of significant harm to an individual.

[*Translation*]

International information-sharing agreements should also provide for minimum privacy safeguards in order to strengthen governance and accountability, and ensure a consistent standard of privacy protection.

Thank you for your work on ensuring stronger protections for Canada's cyber infrastructure while protecting Canadians' fundamental right to privacy. I would now be happy to answer any questions. Thank you.

[*English*]

**The Chair:** Thank you, commissioner.

Commissariat à la protection de la vie privée du Canada pour les nouveaux programmes et les nouvelles initiatives créés grâce aux pouvoirs conférés par le projet de loi C-26 permettrait aussi de renforcer la protection de la vie privée et la confiance de la population canadienne, tout en servant l'intérêt public.

[*Français*]

La réalisation d'une évaluation des facteurs relatifs à la vie privée est actuellement une exigence prévue par la Directive sur les pratiques relatives à la protection de la vie privée du Secrétariat du Conseil du Trésor du Canada, mais elle n'est pas une obligation juridique contraignante sous le régime des lois sur la protection des renseignements personnels. L'évaluation des facteurs relatifs à la vie privée constitue un outil important qui permet de cerner, analyser, traiter et atténuer les problèmes relatifs à la protection de la vie privée avant de mettre en œuvre des initiatives, et ainsi permettre de réduire les préjudices involontaires à la vie privée lors du lancement de ces initiatives. C'est pourquoi j'ai recommandé que la réalisation d'une évaluation des facteurs relatifs à la vie privée devienne une obligation juridique contraignante pour le gouvernement, au titre de la Loi sur la protection des renseignements personnels.

[*Traduction*]

Le projet de loi reconnaît l'importance de la collaboration entre les homologues nationaux et internationaux pour veiller à ce que les infrastructures essentielles soient protégées contre diverses menaces. Afin de renforcer davantage cette collaboration, le Commissariat devrait également être informé des cyberincidents qui pourraient entraîner une atteinte importante à la vie privée. Il pourrait s'agir d'être informé par le Centre de la sécurité des télécommunications chaque fois que ce dernier reçoit un rapport portant sur un cyberincident qui pourrait présenter un risque réel de préjudice grave pour une personne.

[*Français*]

Par ailleurs, les ententes internationales d'échange de renseignements personnels devraient également prévoir des mesures minimales de protection, afin de renforcer la gouvernance et la responsabilité et d'assurer une norme uniforme de protection de la vie privée.

Je tiens à vous remercier de votre travail en vue d'assurer une meilleure protection de l'infrastructure cybernétique du Canada, tout en protégeant le droit fondamental des Canadiennes et des Canadiens à la vie privée. Je serai heureux de répondre à vos questions. Merci.

[*Traduction*]

**Le président :** Merci, monsieur le commissaire.

[*Translation*]

**The Honourable Simon Noël, K.C., Intelligence Commissioner, Office of the Intelligence Commissioner:** Thank you, Mr. Chair and senators.

[*English*]

My comments today are informed by my legal and judicial background, including my time as designated judge of the Federal Court, and by my experience as Intelligence Commissioner. In one sentence, my mandate, as I see it, is to approve, or not, certain national security activities planned by CSE and CSIS and authorized by their respective ministers.

In that sense, the Intelligence Commissioner fulfills an oversight role, as opposed to a review role. My approval is required before the activities can be conducted. The Intelligence Commissioner's approval is necessary because the activities the minister authorizes may be contrary to the law or breach the reasonable expectation of privacy of Canadians. My job is to ensure that the minister has struck an appropriate balance between the national security objectives, on the one hand, and the Charter and important privacy rights on the other.

[*Translation*]

I support the objectives of the bill. In my work, I see the usefulness and advantages of a national approach to effective governance of cybersecurity activities. However, I have a few comments to share with you. My duties as commissioner include approving ministerial security authorizations aimed at non-federal entities deemed important by the federal government. Some examples are the health care and energy sectors.

A non-federal institution can ask for help or support with cybersecurity from the Communications Security Establishment Canada. If the cybersecurity activities the CSE wants to undertake in support of the non-federal entity could violate the law or lead to information gathering that infringes on Canadians' lives, the minister needs to authorize the activities. If necessary, I then need to approve the authorization.

[*Français*]

**L'honorable Simon Noël, c.r., commissaire au renseignement, Bureau du commissaire au renseignement :** Merci, monsieur le président, mesdames les sénatrices et messieurs les sénateurs.

[*Traduction*]

Mes commentaires d'aujourd'hui s'appuient sur mon expérience dans les domaines juridique et judiciaire, notamment à titre de juge désigné de la Cour fédérale, et sur mon expérience en tant que commissaire au renseignement. En une phrase, mon mandat en tant que commissaire au renseignement consiste à approuver, ou non, certaines activités de sécurité nationale planifiées par le Centre de la sécurité des télécommunications, ou CST, et le Service canadien du renseignement de sécurité, ou SCRS, et autorisées par leurs ministres responsables.

En ce sens, le commissaire au renseignement assume un rôle de surveillance plutôt qu'une fonction d'examen. Mon approbation est requise avant que les activités puissent être menées. L'approbation du commissaire au renseignement est nécessaire parce que les activités que le ministre autorise peuvent être contraires à la loi ou porter atteinte aux attentes raisonnables de protection en matière de vie privée des Canadiens. Mon travail est de m'assurer que le ministre a trouvé un juste équilibre entre les objectifs de sécurité nationale, d'une part, et la Charte et les droits importants en matière de vie privée, d'autre part.

[*Français*]

J'appuie les objectifs du projet de loi. Dans le cadre de mon travail, je constate l'utilité et les avantages d'une approche nationale pour une gouvernance efficace des activités de cybersécurité. Toutefois, j'ai quelques commentaires à partager avec vous. En tant que commissaire, je dois notamment approuver des autorisations de sécurité ministérielles qui visent des entités non fédérales qui ont été désignées comme étant importantes par le gouvernement fédéral. Par exemple, on peut penser aux secteurs de la santé ou de l'énergie.

Une institution non fédérale peut demander de l'aide ou du soutien au Centre de la sécurité des télécommunications Canada en matière de cybersécurité. Si les activités de cybersécurité que le Centre de la sécurité des télécommunications Canada souhaite entreprendre pour appuyer l'entité non fédérale risquent de contrevenir à une loi ou peuvent mener à la collecte d'informations qui briment la vie des Canadiens, le ministre doit autoriser les activités. S'il le faut, je dois ensuite approuver l'autorisation.

[*English*]

When I review ministerial cybersecurity authorizations, my primary concern is that the breach of privacy rights is justified, which means that it is necessary and proportionate, and that there are equal measures in place to limit the impact on the privacy of Canadians. The CSE does not target the collection of personal information of Canadians when it comes to cybersecurity; however, there can nevertheless be a reasonable expectation of privacy even in technical information, as confirmed by the Supreme Court last March.

In my experience as the Intelligence Commissioner, when the CSE conducts cybersecurity activities, there will be a collection of information in which there is a reasonable expectation of privacy. This means there is effectively a seizure of private information. If I approve the ministerial authorization, it is because the correct balance has been struck.

Certain elements of Bill C-26 highlight how the treatment of ministerial orders are different than in the context of the Communications Security Establishment Act. In Bill C-26, there is no pre-approval of activities where those activities may be contrary to the law. In particular, there are two areas I want to highlight for your consideration. First, the proposed clause 15.4 of the Telecommunications Act allows the minister to essentially compel the production of any information in support of orders. This information could include personal information which, under broad exceptions, could then be widely disclosed. Second, as you have heard other witnesses say, Part 2, clause 32, allows for the regulators to carry out the equivalent of unwarranted searches where, again, personal information could be collected.

[*Translation*]

The glaring absentee in this bill is the Canadian public. The information that is collected is Canadians' personal information.

Whether under Part 1 or Part 2, the CSE will play a crucial role and possess information, technical or otherwise, for which there is a reasonable expectation of privacy.

[*Traduction*]

Lorsque j'examine une autorisation ministérielle en matière de cybersécurité, ce qui m'importe avant tout, c'est que l'atteinte aux droits à la vie privée soit justifiée. Autrement dit, elle doit avoir un caractère nécessaire et proportionnel, et il y doit y avoir des mesures adéquates en place pour limiter toute incidence sur la vie privée des Canadiens. Lorsqu'il mène des activités de cybersécurité, le CST ne cible pas la collecte de renseignements personnels sur les Canadiens. Toutefois, il peut y avoir une attente raisonnable de protection en matière de vie privée même lorsqu'il est question de renseignements techniques — comme l'a confirmé la Cour suprême du Canada en mars dernier.

D'après mon expérience à titre de commissaire au renseignement, lorsque le CST mène des activités de cybersécurité, il recueille des renseignements pour lesquels il existe une attente raisonnable en matière de respect de la vie privée. Cela signifie que des renseignements personnels sont effectivement saisis. Si j'approuve l'autorisation ministérielle, c'est parce que le juste équilibre a été trouvé.

Certains éléments du projet de loi C-26 soulignent à quel point le traitement des arrêtés ministériels est différent de ce qu'il est dans le contexte de la Loi sur le Centre de la sécurité des télécommunications. Dans le contexte du projet de loi C-26, il n'y a pas d'approbation préalable d'activités qui pourraient être contraires à la loi. Plus particulièrement, il y a deux points que j'aimerais porter à votre attention. Premièrement, le projet d'article 15.4 de la Loi sur les télécommunications permet au ministre, essentiellement, d'exiger la production de toute information à l'appui des arrêtés. Il se peut que cette information comprenne des renseignements personnels qui, en vertu d'exceptions générales, pourraient ensuite être largement diffusés. Deuxièmement, comme vous l'avez entendu d'autres témoins, la partie 2 permet aux organismes de réglementation de mener des activités équivalant à des saisies sans autorisation préalable, où, encore une fois, des renseignements personnels pourraient être recueillis.

[*Français*]

Le grand absent dans ces situations, c'est le public canadien. C'est l'information personnelle des Canadiens qui pourrait faire l'objet de ces collectes.

Que ce soit en vertu de la partie 1 ou de la partie 2, le CST jouera un rôle primordial et sera détenteur de cette information, sous forme technique ou autre, qui contiendra des éléments pour lesquels nous avons une attente raisonnable relative à la vie privée.

[*English*]

In light of the invasive nature of the bill, it is important that meaningful safeguards be part of it so that Canadians have confidence in their cybersecurity system.

[*Translation*]

I will be happy to answer any questions you may have.

[*English*]

**The Chair:** Thank you, commissioner. Next, we'll hear from Mr. Yalkin.

[*Translation*]

**Tolga Yalkin, Assistant Superintendent, Regulatory Response Sector, Office of the Superintendent of Financial Institutions:** Good afternoon, Mr. Chair, ladies and gentlemen of the committee.

It's a privilege to speak with you today about Bill C-26 and its implications for cybersecurity.

Cyber risks are an urgent and growing challenge. Attacks are increasing in both frequency and complexity. They target institutions' operations, compromise sensitive data and, if unchecked, could undermine public trust in Canada's financial system.

[*English*]

At the Office of the Superintendent of Financial Institutions, or OSFI, we are tasked with ensuring the institutions we oversee can withstand threats to their integrity and security. Cyber risks are a key area of focus because they not only disrupt individual organizations but can also ripple across sectors, affecting financial stability.

OSFI has taken a number of significant steps to address cyber risks over the years. First, on risk identification, cyber risk has been a priority in our annual risk outlook that we've published for the last few years. We regularly highlight the growing impact of ransomware, data breaches, and third-party vulnerabilities.

Second, on policy development, we have issued two relevant guidelines for financial institutions: first, guideline B-13 on technology and cyber risk management, which outlines how institutions should manage risks like data breaches and technology outages; and second, on guideline B-10, which

[*Traduction*]

Compte tenu de la nature envahissante du projet de loi, il est important que des mesures de protection significatives en fassent partie afin que les Canadiens aient confiance dans le système de cybersécurité.

[*Français*]

Je serai heureux de répondre à toute question que vous pourriez avoir.

[*Traduction*]

**Le président :** Merci, monsieur le commissaire. Nous allons maintenant entendre M. Yalkin.

[*Français*]

**Tolga Yalkin, surintendant auxiliaire, Secteur des mesures de réglementation, Bureau du surintendant des institutions financières :** Bonjour, monsieur le président et mesdames et messieurs les membres du comité.

C'est un privilège de prendre la parole aujourd'hui au sujet du projet de loi C-26 et de son incidence sur la cybersécurité.

Les cyberrisques représentent un défi urgent et grandissant. Les cyberattaques se multiplient et se complexifient. Elles ciblent les activités des institutions, compromettent leurs données et, en l'absence de contrôles rigoureux, peuvent miner la confiance du public envers le système financier canadien.

[*Traduction*]

Au Bureau du surintendant des institutions financières, ou BSIF, nous avons la tâche de veiller à ce que les institutions sous notre surveillance puissent résister aux menaces à leur intégrité et à leur sécurité. Nous prêtons une attention particulière aux cyberrisques, puisque ces derniers peuvent non seulement entraver les activités des institutions visées, mais aussi se répercuter sur d'autres secteurs et ainsi nuire à la stabilité financière.

Le BSIF a pris des mesures importantes dans trois aspects de la gestion des cyberrisques au fil des ans. Tout d'abord, nous avons agi à l'étape du recensement des risques : toutes les éditions de notre Regard annuel sur le risque que nous avons publiées ces dernières années classaient le cyberrisque comme l'un des axes de priorité. Nous soulignons fréquemment les répercussions de plus en plus importantes des rançongiciels, des fuites de données et des vulnérabilités de tiers.

Ensuite, au chapitre de l'élaboration de politiques, nous avons publié deux lignes directrices pertinentes à l'intention des institutions financières : premièrement, la ligne directrice B-13 sur la gestion du risque lié aux technologies et du cyberrisque, qui explique comment les institutions financières doivent gérer

covers third-party risk management and which addresses risks from third-party service providers, a growing area concern as institutions increasingly rely on external technology.

Third, regarding incident reporting and self-assessment tools, we require financial institutions to report cyber incidents and offer tools like our cybersecurity self-assessment to help them gauge and improve their preparedness.

These measures have helped create a baseline. However, they are not enough on their own. Cyber-threats evolve too rapidly, and gaps remain in the broader ecosystem. A legislative framework like Bill C-26 offers a critical opportunity to strengthen Canada's defences across vital services and sectors.

While OSFI has focused on the financial system, a coordinated national approach is needed to address systemic risks and prevent silos in regulation. We believe this framework can build on existing guidelines to reduce regulatory overlap and address gaps; drive collaboration among regulators, industries and third parties; and foster a culture of resilience, not just prevention, across the system.

Despite these efforts, cybersecurity remains a moving target. Prevention is essential, but institutions must also focus on resilience, on being able to recover swiftly from attacks and maintain critical operations. The question we face is not if incidents will occur but how well we are prepared to respond and recover. This requires ongoing vigilance, innovation and coordination across sectors.

[*Translation*]

In summary, OSFI is committed to doing its part to build a resilient financial system. But the scale and complexity of cyber-threats demand a collective effort. Bill C-26 represents a step forward in aligning Canada's response to these challenges.

I look forward to your questions and to discussing how we can advance this important work together. Thank you.

différents risques, par exemple les fuites de données et les pannes technologiques. Deuxièmement, la ligne directrice B-10 sur la gestion du risque lié aux tiers, qui traite des risques liés aux tiers fournisseurs de services. Il s'agit d'une préoccupation croissante pour nous, car les institutions font de plus en plus appel à des technologies de tiers.

Finalement, il faut se tourner vers les outils de signalement des incidents et les outils d'autoévaluation. Nous demandons aux institutions financières de signaler les cyberincidents et leur offrons des outils, comme l'outil d'autoévaluation en matière de cybersécurité, pour les aider à déterminer et à améliorer leur niveau de préparation.

Ces mesures ont aidé à jeter les bases, mais ne suffisent pas. Les cybermenaces évoluent trop rapidement, et des lacunes existent encore dans l'écosystème général. Un cadre législatif comme le projet de loi C-26 représente une grande occasion de renforcer les défenses du Canada à l'échelle de ses services et secteurs essentiels.

Si le BSIF s'attarde surtout au secteur financier, une approche coordonnée à l'échelle nationale s'impose tout de même pour donner suite aux risques systémiques et éviter un régime de réglementation cloisonné. À notre avis, un tel cadre peut : faire fond sur les lignes directrices existantes afin de réduire les redondances réglementaires tout en corrigeant les lacunes; favoriser la collaboration entre les différents organismes de réglementation, secteurs et tiers; promouvoir une culture de résilience, et non simplement une culture de prévention, à l'échelle du système.

Malgré tous les efforts de contrôle, le domaine de la cybersécurité ne cesse jamais d'évoluer. Bien que la prévention soit cruciale, les institutions doivent aussi faire des efforts pour renforcer leur résilience, c'est-à-dire, pouvoir se rétablir rapidement après une attaque et poursuivre leurs activités essentielles. La question n'est plus de savoir s'il y aura des cyberincidents, mais plutôt de déterminer si nous sommes prêts à y faire face et à nous en remettre. Pour cela, il faut faire preuve de vigilance et d'innovation, et assurer la coordination des efforts à l'échelle des secteurs.

[*Français*]

En résumé, le BSIF est résolu à participer aux efforts en vue de renforcer la résilience du système financier. Cependant, la portée et la complexité des cybermenaces exigent un effort collectif. Le projet de loi C-26 représente un pas dans la bonne direction, vers l'adoption par le Canada d'une approche concertée face à ces défis.

Je serai heureux de répondre à vos questions et de poursuivre la discussion sur les façons d'optimiser la collaboration dans ce dossier important. Merci.

[*English*]

**The Chair:** Thank you, Mr. Yalkin.

We will proceed to questions. As usual, four minutes will be allotted to each question, including the answer. I ask that you keep your questions succinct in an effort to allow as many interventions as possible.

Our first question is from our deputy chair, Senator Dagenais.

[*Translation*]

**Senator Dagenais:** My question is for Mr. Noël and Mr. Dufresne. When Canadian companies like Pratt & Whitney are awarded American military contracts, their employees are subjected to highly stringent security checks. However, they are done by Americans, not Canadians.

I agree that they are our allies, but for years now, we have been forced to let a foreign power into our systems if we want to get contracts.

Some witnesses have raised concerns before the committee about the personal information sharing that could be authorized if Bill C-26 is passed. What do you think of the safeguards put in place to allow both investigations and privacy protection, especially if one of our allies requests information based on unverified suspicions?

**Mr. Dufresne:** That question has been given a great deal of thought internationally.

The Organisation for Economic Co-operation and Development produced a report on government use of personal data held by the private sector in relation to cross-border data flows. That is an aspect we are dealing with in the G7 in terms of data sharing based on trust. Basically, that requires us to have information-sharing protocols with our international counterparts. I signed a protocol with the U.S. Federal Communications Commission, or FCC, on joint investigations and information sharing.

We need to be disciplined when it comes to privacy, which should be treated as a fundamental right. I would also make a few recommendations, such as recognizing that collecting and using information must be necessary and proportional, stating that we won't keep the information longer than necessary and, when sharing information internationally, signing strict information-sharing agreements and putting safeguards in place. Yes, some sharing may be necessary, but privacy needs to be treated as a fundamental right.

[*Traduction*]

**Le président :** Merci, monsieur Yalkin.

Nous allons passer aux questions. Comme d'habitude, quatre minutes seront allouées à chaque question, y compris la réponse. Je vous demande de poser des questions succinctes afin de permettre le plus grand nombre d'interventions possible.

Notre première question est posée par notre vice-président, le sénateur Dagenais.

[*Français*]

**Le sénateur Dagenais :** Ma question s'adresse à MM. Noël et Dufresne. Quand des compagnies canadiennes comme Pratt & Whitney obtiennent des contrats militaires avec les États-Unis, leurs employés sont soumis à des enquêtes de sécurité très rigoureuses. Cependant, ces enquêtes ne sont pas canadiennes; elles sont faites par les Américains.

Je suis d'accord pour dire que ce sont nos alliés, mais depuis plusieurs années, nous avons un étranger dans nos systèmes et nous nous sentons obligés de le laisser faire si nous voulons obtenir les contrats.

Devant le comité, certains témoins ont soulevé des inquiétudes quant au partage d'informations personnelles qui pourrait être autorisé avec l'adoption du projet de loi C-26. Que pensez-vous des balises qui sont mises en place pour permettre, d'une part, d'enquêter et, d'autre part, de respecter la vie privée, surtout si l'on fait face à une demande d'information qui provient de l'un de nos alliés, sur un doute non vérifié?

**M. Dufresne :** Cette question fait l'objet de beaucoup de réflexion au plan international.

L'OCDE a produit un rapport sur l'utilisation par l'État de données personnelles qui sont en possession du privé lors de l'échange transfrontalier de données personnelles. C'est un élément qui nous occupe au sein du G7 et en ce qui concerne l'échange de données basé sur la confiance. Fondamentalement, cela exige que, dans ces échanges d'information, il y ait des protocoles avec les vis-à-vis internationaux. J'ai signé un protocole avec la Commission fédérale des communications (FCC) aux États-Unis sur des enquêtes conjointes et des échanges d'informations.

Il faut avoir une discipline par rapport à la vie privée, que l'on doit traiter comme un droit fondamental. Je ferais aussi certaines recommandations, comme reconnaître la nécessité et la proportionnalité par rapport à la collecte et à l'utilisation, dire qu'on ne va pas maintenir l'information plus longtemps que nécessaire et, lorsqu'on partage de l'information à l'international, conclure des ententes strictes sur le partage d'information et établir des balises. Oui, un certain partage peut être nécessaire, mais il faut toujours le traiter comme étant un droit fondamental.

**Senator Dagenais:** Do you have any comments, Mr. Noël?

**Mr. Noël:** That is a very relevant question. In the current system, under the act that governs it, the CSE needs to comply with very serious internal policies. Let me explain.

In a cyberdefence operation, if information gathering impacts Canadians' privacy, the information may be kept for a maximum of one year, unless it is deemed essential for the purposes of the cyberdefence operation.

As you have seen, personal information can be disclosed under the bill. The exception is very broad and has no parameters for now. The regulations on the way could cover that aspect, but I know that an act is powerful enough to override any regulation. I currently don't see any provision in the bill that ensures the protection of the information of all Canadians, including employees of Pratt & Whitney.

**Senator Dagenais:** My next question is for Mr. Yalkin. We've just outlined the risks of offshore contracting by large Canadian telecoms.

Speaking of which, do financial institutions and insurance companies subcontract part of their activities to companies offshore? If so, do they require security checks on third-party employees with access to sensitive customer service information?

**Mr. Yalkin:** Thank you for the question.

[*English*]

Yes, indeed. We actually have a new guideline on this, which is our integrity and security guideline, which we published last year. It specifically provides for the appropriate background and security checks to be provided on third-party service providers and their employees in circumstances where the risk warrants it.

We operate in a risk-based system, so whether and what is required depends on the circumstances, the nature of the information that is being treated and the access that might be provided to those employees, and based on that, there is a proportional approach to determining what the different security and clearances and background checks are that financial institutions need to ensure are undertaken in order to protect that information.

Much depends on the circumstance that the third-party service provider is being contracted for. I will say that the simple, sheer fact that, indeed, those services are being provided by a third-

**Le sénateur Dagenais :** Vous aviez un commentaire à faire, monsieur Noël?

**M. Noël :** Votre question est très à propos. Dans le système actuel, en vertu de la loi dans laquelle il est impliqué, le CST doit se conformer à des politiques internes très sérieuses. Je m'explique.

Dans le cadre d'une opération de cyberdéfense, s'il y a de la collecte d'information qui touche la vie privée des Canadiens, cette information ne peut être détenue que pour un maximum d'un an, à moins qu'elle puisse être qualifiée d'essentielle pour les fins de l'opération de cyberdéfense.

Quant à la façon de dévoiler de l'information, vous avez vu dans le projet de loi que l'information personnelle peut être dévoilée. L'exception est très large et il n'y a aucun paramètre pour le moment. Il se peut que les règlements à venir couvrent cet aspect, mais ce que je connais de l'importance d'une loi, c'est qu'elle prime sur tout règlement et actuellement, je ne vois aucune disposition dans le projet de loi qui veille à protéger cette information pour tous les Canadiens, y compris les employés de Pratt & Whitney.

**Le sénateur Dagenais :** Ma prochaine question s'adresse à M. Yalkin. On vient d'exposer les risques que représente la sous-traitance étrangère par les grandes compagnies de télécommunications canadiennes.

Par ailleurs, est-ce que les institutions financières et les compagnies d'assurance sous-traitent une partie de leurs activités à l'étranger? Si oui, est-ce qu'elles exigent des enquêtes de sécurité sur les employés des sous-traitants qui ont accès à des informations sensibles dans le cadre du service à la clientèle?

**M. Yalkin :** Je vous remercie de la question.

[*Traduction*]

Oui, en effet. Nous avons publié l'année dernière une nouvelle ligne directrice sur l'intégrité et la sécurité. Elle prévoit notamment qu'il faut effectuer les vérifications d'antécédents et de sécurité appropriées concernant les tiers fournisseurs de services et leurs employés lorsque le risque le justifie.

Nous fonctionnons dans un système fondé sur le risque, donc la question de savoir si des vérifications sont requises dépend des circonstances, de la nature des renseignements traités et de l'accès qui pourrait être accordé à ces employés. Par conséquent, il existe une approche proportionnelle pour déterminer les différentes habilitations de sécurité et vérifications d'antécédents que les institutions financières doivent s'assurer de réaliser afin de protéger ces renseignements.

Tout dépend des circonstances dans lesquelles le tiers fournisseur de services est embauché. Je dirai que le simple fait que ces services soient fournis par un tiers ne dispense pas

party service contractor does not absolve the financial institution from ensuring that the appropriate checks are being conducted.

[*Translation*]

**Senator Carignan:** Thank you. This question is for the head of OSFI. In Canada, there are also service centres, many of them in Montreal, that deal with American institutions. Is Canada more or less strict than other countries, such as France or the U.S., in terms of holding information?

[*English*]

**Mr. Yalkin:** It's a very good question. It's difficult for me to answer that question, because in the interests of full disclosure, I'm not an expert on all of the information and protection requirements that Canadian companies are subject to.

What I can tell you is that when it comes to financial institutions in Canada, whether they're operating in Canada or in other jurisdictions, we have expectations on them when it comes to the protection and the integrity of the data that they collect and hold.

In fact, this is also something that was covered in our recent integrity and security guideline. We outline our expectations for financial institutions on a consolidated basis. Consolidated basis means that their operations, both in Canada and abroad, that they took appropriate precautions to ensure that the integrity of the data that they collect — personal or otherwise — is protected.

[*Translation*]

**Senator Carignan:** This question if for Mr. Dufresne. I know that you're investigating a relatively large data breach at the Canada Revenue Agency. Isn't it a little utopian to think that the government is in a position to issue directions and properly manage that aspect of cybersecurity when it is clearly incapable of doing so for itself?

**Mr. Dufresne:** I think what we're finding is that we need a legal framework where the government is dealt with as stringently as the private sector. Under the act as it stands, the private sector has an obligation to report privacy breaches to my office and to individuals. The public sector is not covered under the act.

**Senator Carignan:** That's unbelievable.

**Mr. Dufresne:** That's in the Treasury Board directive. There are incidents where the privacy breach is reported later. Bill C-26 includes a 72-hour deadline, but the government has an internal policy. One of the recommendations is to make it

l'institution financière de s'assurer que les vérifications appropriées sont effectuées.

[*Français*]

**Le sénateur Carignan :** Merci. Ma question s'adresse au responsable du Bureau du surintendant des institutions financières. Au Canada, on a aussi des centres de service qui desservent des institutions américaines; plusieurs sont à Montréal, notamment. Est-ce qu'on est plus ou moins sévères que les autres pays, que ce soit la France ou les États-Unis, lorsque nous détenons ces informations ici au Canada?

[*Traduction*]

**M. Yalkin :** C'est une très bonne question. Il m'est difficile d'y répondre, car, en toute franchise, je ne connais pas toutes les exigences en matière d'information et de protection auxquelles les entreprises canadiennes sont soumises.

Ce que je peux vous dire, c'est que nous avons des attentes à l'égard des institutions financières au Canada, qu'elles exercent leurs activités au Canada ou dans d'autres pays, en ce qui concerne la protection et l'intégrité des données qu'elles recueillent et conservent.

En fait, c'est aussi un aspect qui a été couvert dans notre récente ligne directrice sur l'intégrité et la sécurité. Nous exposons nos attentes à l'égard des institutions financières, sur une base consolidée. Une base consolidée signifie que, dans le cadre de leurs activités, au Canada et à l'étranger, elles ont pris les précautions appropriées pour garantir la protection de l'intégrité des données personnelles ou autres qu'elles recueillent.

[*Français*]

**Le sénateur Carignan :** Mon autre question s'adresse à M. Dufresne. Je sais que vous enquêtez sur une fuite de renseignements à l'Agence du revenu du Canada qui est assez importante. N'est-ce pas utopique de penser que le gouvernement serait bien placé pour donner des directives et bien gérer cette dimension de la cybersécurité, alors que, manifestement, il n'est pas capable de le faire pour lui-même?

**M. Dufresne :** Je pense que ce que l'on constate, c'est qu'il faut avoir un régime juridique où l'État n'est pas traité moins sévèrement que le secteur privé. En ce moment, en vertu de la loi, le secteur privé a l'obligation de rapporter les atteintes à la vie privée à mon bureau et auprès des individus. Pour ce qui est du secteur public, cela n'est pas dans la loi.

**Le sénateur Carignan :** C'est incroyable.

**M. Dufresne :** C'est dans la directive du Conseil du trésor. On voit des situations où l'atteinte à la vie privée est rapportée plus tard. Dans le projet de loi C-26, on parle d'une durée maximum de 72 heures, mais au sein du gouvernement, on a une

mandatory. We need to update the Privacy Act for the public sector. The act is 40 years old, so it's a priority. That's a prime example.

**Senator Carignan:** Thank you.

[*English*]

**Senator M. Deacon:** Thank you for being here today with us.

I'm going to also ask a question for Mr. Dufresne. Looking through this bill, clauses 26 through 29, it addresses the disclosure and use of information collected under the critical cyber systems protection act, or CCSPA.

While the CCSPA prohibits knowingly disclosing or allowing the disclosure of confidential information, it also creates a list of exceptions, including the disclosure under the Security of Canada Information Disclosure Act, which allows for the disclosure of information among 17 federal departments and agencies.

That's a lot of eyes — maybe ears too — but a lot of eyes that could come across sensitive information. Are you confident our public servants will receive appropriate guidance on how to handle this information, and will you be involved in crafting the regulations or guidelines around them?

**Mr. Dufresne:** Thank you for the question.

Well, I would expect the federal government to consult my office in terms of drafting regulations that have a privacy aspect for Canadians, but at the same time, as was indicated by the Intelligence Commissioner, Mr. Noël, if something is in a regulation, it's not the same thing as if it's in the statute itself.

The recommendation is to ensure that the sharing of information is restricted to the minimum requirement — the necessity and proportionality — that they have ISAs — information sharing agreements — that set out very specifically those requirements and also that the retention be limited. This was something that was introduced at committee in the House. It was not kept after third reading, and so that is a shortcoming.

Now, that said, the Privacy Act will apply to the government departments, but the other element of my recommendation is that my office may not be aware of an issue that's going on if there's confidentiality or if there is a breach. Hence, the recommendation that I included, that if there is a breach that's reported to the CSE, then CSE should be reporting this to my office, and that strengthens our collaboration.

politique. Une des recommandations, c'est de rendre cela obligatoire. Il faut moderniser la Loi sur la protection des renseignements personnels dans le secteur public. Cette loi a 40 ans, donc c'est une priorité. C'est un excellent exemple.

**Le sénateur Carignan :** Merci.

[*Traduction*]

**La sénatrice M. Deacon :** Merci d'être ici aujourd'hui avec nous.

Je vais aussi poser une question à M. Dufresne. Les articles 26 à 29 du projet de loi portent sur la communication et l'utilisation des renseignements recueillis en vertu de la Loi sur la protection des cybersystèmes essentiels, ou LPCE.

La LPCE prévoit que nul ne peut sciemment communiquer des renseignements confidentiels ni en autoriser la communication, mais elle crée également une liste d'exceptions, notamment la communication en conformité avec la Loi sur la communication d'information ayant trait à la sécurité du Canada, qui permet la communication de renseignements entre 17 ministères et organismes fédéraux.

Cela fait beaucoup d'yeux — peut-être aussi beaucoup d'oreilles — mais beaucoup d'yeux qui pourraient tomber sur des renseignements sensibles. Êtes-vous sûr que nos fonctionnaires recevront des conseils appropriés sur la façon de traiter ces renseignements, et participerez-vous à l'élaboration des règlements ou des lignes directrices à ce sujet?

**M. Dufresne :** Merci de la question.

Je m'attends à ce que le gouvernement fédéral consulte mon bureau pour rédiger des règlements qui ont un aspect relatif à la protection de la vie privée des Canadiens, mais en même temps, comme l'a indiqué le commissaire au renseignement, M. Noël, si quelque chose figure dans un règlement, ce n'est pas la même chose que si cela figure dans la loi elle-même.

La recommandation est de veiller à ce que l'échange de renseignements soit limité au minimum requis — la nécessité et la proportionnalité —, qu'il y ait des ententes d'échange de renseignements, ou EER, qui énoncent très précisément ces exigences et que la conservation soit limitée. C'est une mesure qui a été présentée au comité de la Chambre. Elle n'a pas été retenue après la troisième lecture, ce qui constitue une lacune.

Cela dit, la Loi sur la protection des renseignements personnels s'appliquera aux ministères, mais l'autre élément de ma recommandation est qu'il est possible que mon bureau ne soit pas au courant d'un problème qui se produit en cas de confidentialité ou d'atteinte à la sécurité des données. D'où la recommandation que j'ai incluse, à savoir que si une atteinte à la sécurité des données est signalée au CST, le CST devrait la signaler à mon bureau, ce qui renforce notre collaboration.

**Senator M. Deacon:** Thank you very much.

**Senator Dasko:** Actually, my question is a bit of an extension of Senator Deacon's question, just to focus a little bit more on the principles that Mr. Dufresne articulated, necessity and proportionality.

You spoke about privacy assessments and notification. How should these be dealt with? Should they actually be in this bill? I'm trying to understand that a little bit more. Are you saying that they are principles that are already part of this ecosystem, shall we say, that are already carried out in some way?

How do we make sure that these principles apply? Do they already apply? Should they be put into the bill? Do they come in regulations? How do we deal with the issues that you raised?

**Mr. Dufresne:** Thank you. Overall, my recommendation is that it should be in the legislation, to put it in the legislation.

**Senator Dasko:** These principles?

**Mr. Dufresne:** For instance, necessity and proportionality are not in the legislation.

Now, that said, the House did adopt some amendments, and it included a requirement that the order should be reasonable to the gravity of the threat of interference, manipulation and disruption. That goes some way. That's something, for sure.

Necessity and proportionality is a known test. It's the standard that we apply in the privacy world. It ensures that you're focusing, similar to what we do in terms of other fundamental rights, the necessity of the objective and the link to that objective. Is it minimally impairing? Is it contextual? Is it proportionate?

We've applied these frameworks to the pandemic measures. This is a contextual tool. It works. It was highlighted. I think the proportionality concept was mentioned by all three of us so far in the discussion. That should be in the act instead of the one that is there.

Information sharing agreements, you could do that by regulation, but if there is a requirement in the act, it is stronger. Privacy impact assessment needs to be in the law. Right now, it is in a directive of the Treasury Board of Canada, and we see that it's not always complied with.

**Senator Dasko:** It needs to be put in.

**La sénatrice M. Deacon :** Merci beaucoup.

**La sénatrice Dasko :** À vrai dire, ma question va en quelque sorte dans la même veine que la question de la sénatrice Deacon. J'aimerais juste parler un peu plus des principes que M. Dufresne a mentionnés, c'est-à-dire la nécessité et la proportionnalité.

Vous avez parlé des évaluations de la protection de la vie privée et de notifications. Comment devrions-nous aborder ces questions? Devrions-nous vraiment les inclure dans ce projet de loi? J'essaie de comprendre un peu plus les choses. Est-ce que vous dites que ce sont des principes qui font déjà partie de cet écosystème, si on peut dire, et qui sont déjà mis en application, en quelque sorte?

Comment s'assurer de la mise en application de ces principes? Sont-ils déjà mis en application? Devraient-ils être inclus dans le projet de loi? Est-ce qu'il faut créer des règlements pour cela? Comment traiter les enjeux que vous avez mentionnés?

**M. Dufresne :** Merci. De façon générale, je recommande de les mettre dans la loi.

**La sénatrice Dasko :** Ces principes?

**M. Dufresne :** Par exemple, la nécessité et la proportionnalité ne sont pas dans la loi.

Alors, cela dit, la Chambre des communes a adopté certains amendements, et a inclus une obligation selon laquelle le décret doit être raisonnable à la gravité des menaces d'ingérence, de manipulation, de perturbation ou de dégradation. Ce n'est pas rien. C'est sûr que c'est quelque chose.

Le critère de la nécessité et de la proportionnalité est un critère connu. C'est la norme que nous mettons en application en ce qui concerne les renseignements personnels. Tout comme ce que nous faisons pour ce qui est des droits fondamentaux, cette norme garantit la nécessité de l'objectif et le lien avec cet objectif. L'atteinte est-elle minimale? Est-elle contextuelle? Est-elle proportionnelle?

Nous avons appliqué ces cadres aux mesures pandémiques. Il s'agit d'un outil contextuel qui fonctionne. Il a été mis en évidence. Je pense que nous avons tous les trois mentionné le concept de proportionnalité jusqu'ici dans le dialogue. C'est ce concept qui devrait figurer dans la loi à la place du concept qui y figure actuellement.

Pour ce qui est des ententes d'échange de renseignements, vous pourriez créer des règlements, mais une exigence dans la loi permettait de renforcer les choses. Il faut inclure une évaluation des effets sur la vie privée dans la loi. À l'heure actuelle, cette évaluation figure dans une directive du Conseil du Trésor du Canada. Mais nous remarquons qu'elle n'est pas toujours respectée.

**La sénatrice Dasko :** Nous devons l'inclure.

I want to go back to the topic that came up earlier about third-party offshore contractors. This came up in previous sessions and panels today.

Do you have a concern about that and the privacy issues involved?

**Mr. Noël:** Yes. Just to add one point to Bill C-59, the bill that looks at the CSE has this necessity and proportionality. It is in the law. It's not in a regulation.

**Senator Dasko:** My question is about third party, offshore contractors and concerns that were raised in previous panels about potential breaches of confidentiality and privacy. Do you have concerns about those?

**Mr. Dufresne:** It's a principle of privacy law that if we're sharing information with third parties outside of borders, we need to make sure we're putting in place equivalent types of protection. That goes to security. That goes to measures of transfer, the purposes, and so on. So it's important there be rigorous frameworks around that. Another principle is if the government is contracting with the private sector, the government needs to make sure that the private sector that it's using is itself complying with its legal obligations.

**Senator McNair:** My question is for the Office of the Superintendent of Financial Institutions. Listening to what you're talking about in your opening remarks, I'm trying to understand. Could you speak a little bit about how the bill will affect the way you currently operate and how you support financial institutions? Does it give you any tools that you don't already have?

**Mr. Yalkin:** Yes. Thank you for the question. Much remains to be seen because we do know the general framework of the law, but much will turn obviously on the regulation and its implementation.

Our general approach to prudential supervision is that we have a broad jurisdiction to supervise financial institutions according to what we think makes sense from our perspective when it comes to ensuring their safety and stability. On that broad grant of authority, we then develop guidelines, including B-13, that I referred to on cyber and tech risk, which set out our expectations for financial institutions and what they should do in order to manage these risks appropriately.

Je souhaite revenir sur le sujet qui a été mentionné plus tôt concernant les sous-traitants tiers étrangers. Le sujet a été mentionné lors de réunions précédentes et par les témoins aujourd'hui.

Avez-vous des préoccupations à ce sujet et concernant les problèmes liés aux renseignements personnels?

**M. Noël :** Oui. Simplement pour ajouter un point au projet de loi C-59, le projet de loi qui encadre le CST inclut cette nécessité et cette proportionnalité. Cet élément figure dans la loi, pas dans un règlement.

**La sénatrice Dasko :** Ma question concerne les sous-traitants tiers étrangers ainsi que les préoccupations abordées par les groupes de témoins précédents, entourant les atteintes potentielles à la confidentialité et à la protection des renseignements personnels. Avez-vous des préoccupations à cet égard?

**M. Dufresne :** Un principe de la Loi sur la protection de la vie privée, c'est que lorsque nous partageons de l'information avec de tierces parties à l'extérieur des frontières, nous devons veiller à ce que des types de protection équivalents soient mis en place. Cela s'applique à la sécurité. Cela s'applique aux mesures de transfert, aux buts, et ainsi de suite. Il est donc important de mettre sur pied des cadres stricts pour ces éléments. Un autre principe de la loi, c'est que lorsque le gouvernement engage des sous-traitants du secteur privé, il doit veiller à ce que le sous-traitant du secteur privé auquel il fait appel se conforme à ses obligations légales.

**Le sénateur McNair :** Ma question s'adresse au Bureau du surintendant des institutions financières. J'ai écouté ce que vous avez dit dans vos observations liminaires, et j'essaie de comprendre. Comment le projet de loi affectera-t-il votre mode de fonctionnement actuel et comment allez-vous soutenir les institutions financières? Ce projet de loi vous fournit-il des outils dont vous ne disposez pas déjà?

**M. Yalkin :** Oui. Merci de votre question. Il y a encore beaucoup à voir, car nous connaissons le cadre général de la loi, mais beaucoup dépendra évidemment du règlement et de son application.

Pour ce qui est de la surveillance prudentielle, notre approche générale consiste à disposer d'une vaste compétence qui nous permet de surveiller les institutions financières selon ce qui, de notre point de vue, est logique et permet d'assurer leur sécurité et leur stabilité. En nous appuyant sur ces vastes pouvoirs, nous mettons au point des lignes directrices, y compris la ligne directrice B-13, à laquelle j'ai fait référence lorsque j'ai parlé du cyberrisque et du risque lié à la technologie. Ces lignes directrices établissent nos attentes pour les institutions financières et les mesures qu'elles doivent prendre pour gérer ces risques de manière appropriée.

The difference that this bill will bring in for us is this: Rather than that being a prudential supervisory approach, it will actually be a regulatory-enforcement approach that will augment the already robust approach that we have to make sure that these risks are being managed appropriately.

In some sense, it could be helpful because it will bring into sharp contrast to financial institutions what those expectations are for them and what the consequences are for failing to comply with them too. I see opportunity for the regulations — however they are developed — to be integrated in a harmonious way with our existing guidelines and approach to prudential supervision.

**Senator McNair:** Mr. Dufresne, I hear what you're saying, and you both are saying that regulation is not as strong as having it in the legislation, but if this is passed as is, the work will begin during the regulatory process to have safeguards put into place, eventually hoping to get it in the legislation itself or the act, I assume. This legislation is not going to be stagnant or static at any time. As soon as it becomes law, there's a process to ensure that it keeps up with all the risks that are forthcoming. Would you comment on that?

**Mr. Dufresne:** My comment would be that, of course, it's up to Parliament to determine what amendments to put in place or not. You have recommendations, but, yes, the regulatory-making process is also a tool that can be used to bring more precision to the legislation. My recommendation would be to make sure that my office is consulted in that process and that is it is seen to be consulted. It's important that Canadians understand the safeguards and the guardrails and that the precision be broad in terms of information-sharing agreement, in terms of bringing precision to those principles. Certainly, my team and I will stand ready to assist in whatever way we can.

**Senator McNair:** Have you had any discussions at this point with different departments on your expectations?

**Mr. Dufresne:** My expectation, which has been repeated regularly to the government, is that we should be consulted early on new initiatives, including bills. Cabinet confidences have to be managed, of course, but the earlier we are consulted, the better we are able to provide input at the front end.

**Senator McNair:** Thank you.

Voici la différence que ce projet de loi apportera pour nous : plutôt qu'une approche de surveillance prudentielle, cette approche sera en fait une approche d'application de la réglementation. Celle-ci augmentera l'approche déjà robuste existante afin de garantir la gestion appropriée de ces risques.

D'une certaine façon, cette approche peut être utile, car elle permettrait de rapidement rehausser les attentes pour les institutions financières et de leur faire comprendre les conséquences qu'elles risquent de subir si elles ne respectent pas, elles aussi, ces attentes. Je vois que nous pouvons créer des règlements, — quelle que soit la façon dont ils sont mis au point — que nous pouvons intégrer de façon harmonieuse dans nos lignes directrices existantes et notre approche liée à la surveillance prudentielle.

**Le sénateur McNair :** Monsieur Dufresne, je comprends ce que vous dites, et vous dites tous les deux que l'inclusion dans le règlement n'est pas aussi solide que l'inclusion dans la loi. Mais si nous adoptons cette loi telle qu'elle, des mesures de protection seront mises en place lors du processus réglementaire, et, au bout du compte, j'espère que nous pourrons inclure ces mesures dans le projet de loi proprement dit ou dans la loi, je suppose. À aucun moment, cette loi ne sera stagnante ou statique. Aussitôt que la loi entrera en vigueur, un processus sera mis en place pour veiller à ce qu'elle surveille de près les risques à venir. Pouvez-vous commenter?

**M. Dufresne :** Je dirais que, bien entendu, il revient au législateur de déterminer quels amendements mettre en place ou non. Vous avez des recommandations, mais effectivement, le processus réglementaire est également un outil susceptible d'apporter davantage de précisions à la loi. Je recommanderais de consulter mon bureau lors de ce processus et de s'assurer qu'on voit qu'il a été consulté. Il est essentiel que les Canadiens comprennent les mesures de protection et de sécurité, et que la précision de l'entente d'échange de renseignements soit large, dans la mesure où ces principes doivent faire l'objet de davantage de précisions. Bien entendu, mon équipe et moi-même serons prêts à vous prêter main-forte par tous les moyens possibles.

**Le sénateur McNair :** Avez-vous discuté jusqu'ici de vos attentes avec différents ministères?

**M. Dufresne :** Mon attente, que nous avons régulièrement répétée au gouvernement, est que nous devrions être consultés tôt dans le processus au sujet des nouvelles initiatives, y compris les projets de loi. Bien entendu, il faut tenir compte des documents confidentiels du Cabinet, mais plus nous sommes consultés tôt et plus nous sommes à même de collaborer en amont.

**Le sénateur McNair :** Merci.

**Senator Batters:** Mr. Dufresne, right on that point, then, when did the government consult you on Bill C-26?

**Mr. Dufresne:** I don't believe we were consulted in the drafting part of that bill.

**Senator Batters:** Not at all?

**Mr. Dufresne:** We made recommendations at the House stage, and a number of them were reflected.

**Senator Batters:** At committee. Thank you, wow, that is a little shocking.

Dealing with some important issues here, your office is able to initiate investigations and to review compliance with the Privacy Act, and there are certain sections in Bill C-26 that allow your office to initiate investigations at your discretion, but as you were saying in your opening remarks, you're recommending that your office should be notified about cybersecurity incidents where a real risk of a privacy breach occurs, because as we've heard about this bill, there could be situations where you never know about it. Unless that recommendation is actually put into effect in the bill, how would you know that you need to initiate an investigation? Is that your concern about this?

**Mr. Dufresne:** Well, it is. To be clear, we have great working relationships with the Communications Security Establishment Canada, but when you're talking about confidential information or breach reports, there is going to be reluctance to sharing that unless you have legal authority to do so. I would be reluctant to do the same. That's why in this instance it would be important that the bill be amended to provide this clear authority to our colleagues at the CSE because privacy and cybersecurity have this in common: They're both built on the principle of safeguarding the information that you have commensurate to the risk and commensurate to the context. So we have a lot to learn from each other. We work very well together, but in this instance, my worry is that we're not going to know, and CSE is not being to be able to tell us. That is a loss for Canadians because they can't have this privacy prism on that.

**Senator Batters:** Absolutely. My next question is to the Intelligence Commissioner. Thank you very much for being here. In my second reading critic speech I was quoting from Professor Malone, who was talking about the legislation for the CSE, and his quote was saying that Bill C-26's provisions diverge markedly from the thrust of the CSE's enabling legislation, because under that legislation, where CSE's spying activities contravene federal law or interfere with the reasonable

**La sénatrice Batters :** Monsieur Dufresne, sur ce sujet exactement, quand est-ce que le gouvernement vous a consulté au sujet du projet de loi C-26?

**M. Dufresne :** Je ne pense pas que nous ayons été consultés lors de l'élaboration de ce projet de loi.

**La sénatrice Batters :** Pas du tout?

**M. Dufresne :** Nous avons fourni des recommandations lorsque le projet de loi était devant la Chambre des communes, et un certain nombre de ces recommandations ont été retenues.

**La sénatrice Batters :** Au comité. Merci. Eh bien, c'est un peu choquant.

En ce qui concerne certains problèmes graves ici, votre bureau est capable de lancer des enquêtes et de procéder à des examens de conformité avec la Loi sur la protection des renseignements personnels, et certains articles du projet de loi C-26 permettent à votre bureau de lancer des enquêtes à votre discrétion. Mais comme vous l'avez mentionné dans vos observations liminaires, vous recommandez que votre bureau soit informé des incidents en matière de cybersécurité lorsqu'un risque réel d'atteinte èa la protection des renseignements personnels a lieu, car, comme nous l'avons vu concernant ce projet de loi, il y a des situations dont vous n'êtes jamais au courant. À moins que cette recommandation soit incluse dans le projet de loi, comment sauriez-vous qu'il faut entreprendre une enquête? Est-ce que c'est quelque chose qui vous préoccupe?

**M. Dufresne :** Eh bien, oui, effectivement. Pour être clair, nous entretenons d'excellentes relations professionnelles avec le Centre de la sécurité des télécommunications Canada, mais lorsqu'il s'agit de renseignements confidentiels ou de rapports sur les atteintes, il y aura de la réticence à partager ces informations, à moins que vous n'ayez le pouvoir légal de le faire. Je serais également réticent à partager ces informations. C'est pourquoi, dans ce cas, il est important que le projet de loi soit amendé afin de fournir ce pouvoir légal clair à nos collègues du CST, car la protection des renseignements personnels et la cybersécurité ont une chose en commun : elles sont toutes deux fondées sur le principe de protection des informations correspondant au risque et au contexte. Nous travaillons très bien ensemble, mais dans ce cas, ma crainte est que nous ne soyons pas informés, et le CST n'est pas capable de nous le dire. C'est une perte pour les Canadiens, car ils n'ont pas ce point de vue axé sur la protection des renseignements personnels.

**La sénatrice Batters :** Absolument. Ma prochaine question s'adresse au commissaire au renseignement. Merci beaucoup d'être ici. Dans le discours que j'ai prononcé à titre de porte-parole à l'occasion de la deuxième lecture, j'ai mentionné une citation de M. Malone, qui parlait du projet de loi au nom du CST, et d'après cette citation, les dispositions du projet de loi C-26 divergent sensiblement de l'idée maîtresse de la loi habilitante du CST. En effet, aux termes de cette loi, advenant la

expectation of privacy for individuals in Canada, the agency must obtain approval from your office, the Office of the Intelligence Commissioner. Last year, the commissioner — he said — fully granted half of such requests: three out of six. The cybersecurity direction powers in Bill C-26 are subject to no similar kind of review.

As you were saying earlier, that is an after-the-fact thing. Unlike what has existed with the CSE situation, they would have to obtain your approval before it happens. If you could speak a little bit more about how your office is involved in those types of situations, and how it differs from what would potentially be the case under Bill C-26 if it wasn't amended at all.

**Mr. Noël:** Thank you, senator. We are involved right from the beginning. We review the minister's decision. We review the chief of CSE's application. We comment on it. We agree sometimes, and sometimes we disagree. You should also know that there is a document that establishes parameters within the CSE. For instance, it will do so on disclosure. It will do so on what is Canadian information, to what extent you should keep that information and how long you're going to keep it. The provisions are such, senator, now that the data received from the cyber-suppliers is looked at carefully.

How do we become involved? We ensure the law is followed. Do you have the jurisdiction to do this — yes or no? We came to the conclusion in a few cases that they were outside their jurisdiction. So that was taken out.

When it comes to private information, we establish some guidelines with these policies, we make remarks, and we have an ongoing communication with the chief of CSE.

Without disclosing anything, it is important to realize that CSE is doing its best, but it's not perfect. When I say this, I think the chief of CSE knows what I'm talking about. I think the fact that we're involved at that stage — we're a bit like the person looking above the shoulder of the decision maker — *un chien de garde* like we say in French — and we then make sure they comply. If they don't, they report back to us, and we ensure that there are proper steps to be followed. That's the type of relationship that we're adding.

**Senator Batters:** And just to be clear, none of that is required under Bill C-26.

**Mr. Noël:** None of that.

violation d'une loi fédérale ou de l'attente raisonnable de respect de la vie privée des citoyens du Canada dans le cadre des activités d'espionnage du CST, l'organisme doit obtenir l'approbation de votre bureau, c'est-à-dire, le Bureau du commissaire au renseignement. L'année dernière, le commissaire a dit avoir accueilli la moitié de ces demandes, c'est-à-dire trois sur six. Les pouvoirs de direction en matière de cybersécurité dans le projet de loi C-26 ne sont pas assujettis à des types d'examens similaires.

Comme vous l'avez mentionné plus tôt, c'est une chose qui se produit après coup. Contrairement à ce qui existait dans le cas du CST, ils doivent demander votre approbation avant que cela se produise. Pouvez-vous parler un peu plus de la façon dont votre bureau gère ce genre de situations, et en quoi cela diffère de ce qui pourrait potentiellement se passer aux termes du projet de loi C-26, advenant qu'il ne soit pas amendé?

**M. Noël :** Merci, madame la sénatrice. Nous intervenons dès le début. Nous examinons la décision du ministre. Nous examinons la demande du chef du CST. Nous la commentons. Parfois, nous sommes d'accord, et parfois, non. Vous devez également savoir qu'il y a un document qui établit les paramètres au sein du CST. Par exemple, ce document établit des paramètres concernant la divulgation. Il établit les paramètres de ce qui constitue de l'information canadienne, et dans quelle mesure cette information devrait être conservée ainsi que la durée pendant laquelle elle devrait l'être. Les dispositions sont telles, madame la sénatrice, qu'à présent, les données reçues par les cyberfournisseurs sont examinées soigneusement.

Comment intervenons-nous? Nous veillons au respect de la loi. Avez-vous la compétence pour le faire — oui ou non? Nous avons conclu que, dans certains cas, certains organismes n'avaient pas la compétence pour le faire, donc, nous les avons retirés.

En ce qui concerne l'information privée, nous avons mis au point des lignes directrices avec ces politiques, nous avons fourni des remarques, et nous communiquons de façon continue avec le chef du CST.

Je ne vais rien révéler, mais il est important de réaliser que le CST fait de son mieux, mais ce n'est pas parfait. Quand je dis cela, je pense que le chef du CST sait de quoi je parle. Je pense que le fait que nous intervenions à cette étape — nous sommes un peu comme la personne qui regarde par-dessus l'épaule du décideur — un chien de garde, comme on dit — et nous voulons veiller au respect de la loi. Si les gens ne respectent pas la loi, ils nous avisent, et nous faisons en sorte de prendre les mesures appropriées. C'est le type de relation que nous ajoutons.

**La sénatrice Batters :** Et juste pour que ce soit clair, rien de tout cela n'est requis aux termes du projet de loi C-26.

**M. Noël :** Absolument rien.

**Senator Batters:** None of that. Thank you.

**Senator LaBoucane-Benson:** My question is for Commissioner Noël. Thank you so much for your testimony.

Perhaps you can help me understand how Bill C-26 operates in a broader legal context. For example, under Bill C-26, Charter protection against unreasonable search and seizure still applies, right? Also Criminal Code prohibition of interception of private communication still applies, right? Can you speak to that, please?

**Mr. Noël:** The Charter still applies, as does section 8 regarding seizures among other things. In all cases I've known, you need a warrant. You can obtain it from the justice of the peace, you can obtain it from the Federal Court, and you can obtain from a quasi-judicial officer. In the present bill, there is no such warrant requirement — except for dwellings or *maison d'habitation*. They make that exception. Everything else, when they go into the office of one of the regulators, the regulator will be able to go in and get what he wants. Normally, that would go against the Charter.

I've read the Charter Statement by the minister, and I haven't seen anything in that statement that would give a justification under section 1 of the Charter. I haven't seen anything. It's a first in Canada where anyone can go and search. And the Supreme Court of Canada is very private about this information. In this case, it's totally absent.

[*Translation*]

**Senator Dagenais:** Mr. Dufresne, I'll go back to information sharing with other countries. Have all the countries in the Five Eyes alliance, meaning our closest allies, agreed in writing to the principle you're talking about? If not, which are not yet part of the privacy agreement? Are there any that are not part of it?

**Mr. Dufresne:** The example I'll give you is the U.K.'s approach, which recommends the idea of proportionality. It can be used as an example for cybersecurity-related information and information sharing with the authorities: It has to be relevant, necessary and proportional. I think that's an example we should follow.

Our European counterparts, because of their obligations, require that the authorities in charge of data protection be notified whenever there is a cybersecurity breach. The data protection authority in Canada is my office, hence my recommendation that we should follow that stricter example. In

**La sénatrice Batters :** Absolument rien. Merci.

**La sénatrice LaBoucane-Benson :** Ma question s'adresse au commissaire Noël. Merci beaucoup de votre témoignage.

Peut-être pourriez-vous me faire comprendre la manière dont le projet de loi C-26 s'applique dans un contexte juridique plus large. Par exemple, aux termes du projet de loi C-26, la protection assurée par la Charte contre les fouilles, les perquisitions et les saisies abusives s'applique-t-elle toujours? L'interdiction imposée par le Code criminel d'intercepter les communications privées s'applique-t-elle toujours? Pourriez-vous nous en dire plus sur le sujet, s'il vous plaît?

**M. Noël :** La Charte est toujours en vigueur, ce qui comprend l'article 8 concernant les saisies, entre autres. Dans tous les cas que j'ai observés, il faut un mandat. Il est possible d'en obtenir un par l'entremise d'un juge de paix, de la Cour fédérale ou d'un officier quasi judiciaire. Dans le présent projet de loi, il n'y existe pas de telles exigences en lien avec le mandat — sauf pour les maisons d'habitation ou les *dwellings*. Une exception est faite dans ces cas. Sinon, lorsque le bureau d'un organisme réglementaire fait l'objet d'une perquisition, le responsable de l'organisme réglementaire en question pourrait entrer dans son bureau et y prendre ce qu'il veut. En temps normal, cela irait à l'encontre de la charte.

J'ai lu l'énoncé concernant la charte émis par le ministre, et je n'ai pas observé quoi que ce soit dans cet énoncé qui fournirait une justification aux termes de l'article premier de la charte. Je n'ai rien vu de tel. Il s'agit de la première fois au Canada que n'importe qui peut entreprendre une fouille. La Cour suprême du Canada est très secrète à propos de ces informations. Dans le cas présent, c'est totalement absent.

[*Français*]

**Le sénateur Dagenais :** Monsieur Dufresne, je vais revenir sur le partage d'information avec d'autres pays. Est-ce que tous les pays du Groupe des cinq, c'est-à-dire nos principaux alliés, ont adhéré par écrit au principe dont vous nous parlez? Sinon, qui ne fait pas encore partie de l'accord sur la vie privée? Est-ce qu'il y en a qui n'en font pas partie?

**M. Dufresne :** Ce que je vais vous donner comme exemple, en fait, c'est que la Grande-Bretagne a une approche où l'on recommande justement la notion de proportionnalité. On peut les citer comme exemple avec l'information liée à la cybersécurité et le partage d'information avec les autorités; il faut que ce soit pertinent, nécessaire et proportionnel. Je crois que c'est un exemple que l'on devrait suivre.

Nos collègues européens, à cause de leurs obligations, vont demander que les autorités qui s'occupent de la protection des données soient avisées quand il y a une atteinte à la cybersécurité. Les autorités de protection des données, c'est mon bureau au Canada, d'où ma recommandation selon laquelle on

the U.S., there are obligations to publish mandatory orders for dealing with privacy and civil rights and freedoms. Once again, that could be reinforced at the regulatory level. This whole matter of holding information…. As I said, we recently signed an agreement with the FCC, in the U.S., a memorandum of understanding. We worked closely with them. I would say that the principles we are advocating are generally accepted when it comes to privacy.

**Senator Dagenais:** Thank you.

[*English*]

**Senator Batters:** Back to the Privacy Commissioner, Mr. Dufresne. At the House of Commons committee, you testified this:

> As drafted, these powers are broad. In order to ensure that personal information is protected and that privacy is treated as a fundamental right, I would recommend that the Committee consider making the thresholds for exercising these powers more stringent, and placing stricter limits on the use of those powers.
>
> One way of doing so would be to require that any collection, use, or disclosure of personal information be both necessary and proportionate. This is a core principle for the handling of personal information that is recognized internationally.

You've talked about this today as well.

Now, the House of Commons committee did pass amendments which explicitly defined personal and de-identified information as confidential, which helps, but there is certainly more to be done to address the serious privacy concerns in this legislation. Please tell us why you don't think the House of Commons amendments go far enough.

**Mr. Dufresne:** Thank you, senator. Indeed, there have been some improvements with the amendments made at the house. You mentioned some with the notion of defining personal information and de-identified information as confidential information for the Telecommunications Act part of Bill C-26. That wasn't done for the other part in terms of confidential information, so there could be clarifications there.

devrait suivre cet exemple plus rigoureux. Aux États-Unis, il y a des obligations pour ce qui est de publier des ordonnances obligatoires pour traiter de la question de la vie privée et des droits et des libertés civiles. Encore une fois, c'est ce qui pourrait être renforcé sur le plan des règlements. Toute cette question de la rétention de l'information... Comme je l'ai dit, on a signé récemment une entente avec la FCC aux États-Unis, un protocole d'entente, donc on travaille de près avec eux. Je dirais que ces principes qu'on met de l'avant sont généralement reconnus en matière de vie privée.

**Le sénateur Dagenais :** Merci beaucoup.

[*Traduction*]

**La sénatrice Batters :** Revenons au commissaire à la Protection de la vie privée, M. Dufresne. Au comité de la Chambre des communes, vous avez déclaré que :

> Selon le projet tel qu'il est rédigé, ces pouvoirs sont larges. Afin de s'assurer que les renseignements personnels sont protégés et que la vie privée est traitée comme un droit fondamental, je recommanderais au comité d'envisager de resserrer les seuils qui encadrent l'exercice de ces pouvoirs et d'imposer des limites plus strictes à l'utilisation de ces pouvoirs.
>
> Pour ce faire, on pourrait exiger que toute collecte, utilisation et communication des renseignements personnels respecte les principes de nécessité et de proportionnalité. Il s'agit de principes de base du traitement des renseignements personnels qui sont reconnus à l'échelle internationale.

Vous avez également abordé cela aujourd'hui.

Le comité de la Chambre des communes a effectivement adopté des amendements qui définissent explicitement les informations personnelles et dépersonnalisées comme étant confidentielles, ce qui est d'une certaine aide, mais il reste assurément de l'ouvrage à faire pour répondre aux grandes préoccupations relatives à la protection de la vie privée au sein du projet de loi. S'il vous plaît, dites-nous en quoi, à votre avis, les amendements de la Chambre des communes sont insuffisants.

**M. Dufresne :** Merci, madame la sénatrice. En effet, quelques améliorations ont été apportées aux amendements proposés au sein de la Chambre. Vous en avez mentionné quelques-unes lorsque vous avez abordé la définition des informations personnelles et dépersonnalisées comme des informations confidentielles dans la partie concernant la Loi sur les télécommunications du projet de loi C-26. Cela n'avait pas été fait pour l'autre partie en ce qui a trait à l'information confidentielle, alors quelques clarifications pourraient être apportées à cet égard.

There have been improvements in terms of the discretion to the minister and Governor-in-Council. The first version was much more "in the opinion of" and now there has been strengthened language about reasonableness, "reasonable to the gravity of the threat." Nonetheless, I continue to recommend the gold standard of necessity and proportionality be the one used.

I think that when you have a standard that is known, that is understood, it's better to continue to use it rather than create a new one. There is a risk that if there is a choice to use different language, people will ask why the legislator did that. Is it to have a less stringent standard?

So the recommendation is that we should stick with those principles. Privacy is a fundamental right. It is not an obstacle to public interest, but Canadians will be reassured by seeing this twin notion of necessity and proportionality overall for personal information.

**Senator Batters:** Thank you. Also with respect to that amendment that was passed by the House of Commons committee but then pulled out at third reading stage in the House of Commons, can you please tell us a little bit more about that, why it actually is important to have that amendment in there and maybe why it would have been pulled out? That's kind of an unusual situation.

**Mr. Dufresne:** Yes. Thank you. This was an amendment that would provide that information shared with departments be kept no longer than necessary for the purpose, to the investigation and so on. This was a privacy protective principle of retention, and it was deleted at third reading.

My understanding is it may have been an understanding that there is a retention principle under the Privacy Act so you could deal it under the Privacy Act. Currently, the Privacy Act regulations don't provide a maximum retention period. It provides a minimum retention period of two years. There remains a gap, and in this instance, the amendment put at second reading, in my view, was a good one, especially if the necessity and proportionate will not be the framework.

**Senator Batters:** Right, because as you were saying the Privacy Act would not cover that. Perhaps they were thinking it did, but you're confirming today that the Privacy Act does not cover that.

Il y a également eu des améliorations quant au pouvoir discrétionnaire conféré au ministre et au gouverneur en conseil. Dans la première version, des termes comme « selon l'avis de » étaient très présents, mais maintenant qu'un libellé plus fort conférant un certain caractère raisonnable a été implanté, on retrouve plutôt des descriptions comme « raisonnable à la gravité des menaces ». Néanmoins, je continue à recommander l'usage de la référence absolue de nécessité et de proportionnalité.

J'estime que lorsque vous utilisez une référence qui est connue et qui est comprise, il vaut mieux continuer à l'utiliser au lieu d'en créer une nouvelle. S'il y a l'option de choisir un libellé différent, nous courons le risque que les gens se demandent pourquoi le législateur a fait cela. Est-ce que c'est pour que la norme soit moins stricte?

Il est donc recommandé que nous nous en tenions à ces principes. La protection de la vie privée est un droit fondamental. Ce n'est pas un obstacle à l'intérêt public, mais les Canadiens seront rassurés de voir que cette notion double de nécessité et de proportionnalité s'applique de manière générale aux renseignements personnels.

**La sénatrice Batters :** Merci. De plus, quant à l'amendement qui a été adopté par le comité de la Chambre des communes, puis qui a été retiré à l'étape de la troisième lecture à la Chambre, pourriez-vous s'il vous plaît nous en dire plus sur l'importance de cet amendement et peut-être aussi la raison pour laquelle il a été retiré? Il s'agit d'une situation plutôt inhabituelle.

**M. Dufresne :** Oui. Merci. Il s'agissait d'un amendement qui garantirait que l'information partagée avec les ministères ne serait pas conservée plus longtemps que nécessaire, à des fins d'enquêtes et ainsi de suite. Il s'agissait d'un principe de conservation des renseignements dans une optique de protection de la vie privée, et il a été supprimé à la troisième lecture.

De ce que j'ai compris, certains auraient pu avoir l'impression qu'il existait déjà un principe de conservation aux termes de la Loi sur l'accès à l'information et la protection de la vie privée, et que le principe de la conservation des renseignements serait effectivement appliqué selon la Loi sur l'accès à l'information et la protection de la vie privée. À l'heure actuelle, le règlement d'application de la Loi sur l'accès à l'information et la protection de la vie privée ne prévoit pas une période de conservation maximale. Il prévoit cependant une période de conservation minimale de deux ans. Un écart demeure, et dans ce cas-là, l'amendement ajouté à la seconde lecture, à mon avis, était pertinent, surtout si le cadre de la nécessité et de la proportionnalité n'est pas en place.

**La sénatrice Batters :** D'accord, car comme vous l'avez mentionné plus tôt, la Loi sur l'accès à l'information et la protection de la vie privée ne s'y applique pas. Peut-être que certains croyaient le contraire, mais vous confirmez aujourd'hui

**Mr. Dufresne:** It would not cover it. You may include it by amending regulations and providing some further detail there. There may be some possibilities, but, again, in this instance, you have the legislation that is providing for these powers and bringing this clarity. There is an opportunity to do this now. I don't want to presume when the Privacy Act will be amended so you have the opportunity to.

**Senator Batters:** When was the last time the Privacy Act was amended? Was that Bill C-15?

**Mr. Dufresne:** It's 40 years old. There may have been some small amendments during this period, but, certainly, it's overdue.

**Senator Batters:** Thank you.

**The Chair:** Colleagues, there are no other senators on the list, so I have a question for Mr. Noël.

You have an important role as the chief Intelligence Commissioner. Given your responsibility of being a guardian of some fundamental principles and values in our democracy when the state should intervene and what the balance is — every time you've been here you have spoken about that balance very eloquently. In this situation, in this bill, your role and responsibility has diminished in how you get to play or continue to play that role. Can you explain to me why that is?

**Mr. Noël:** I have no reason why the conceptualizers of this bill have decided to — I haven't been consulted. I haven't been briefed on it. Although, just a few days ago they made an offer, which I declined, because I'm an independent officer. I don't know why they have decided to put this oversight apart.

**The Chair:** Given the extremely important responsibility of cybersecurity for the whole nation, not just for individuals, there is always going to be a balance that needs to be struck in the interest of the country, protecting Canadians and institutions in many places, but wouldn't it be fair for Canadians to want to understand whenever there is a need to find some way to deal with the gravity of the situation, we would have somebody providing oversight, which you have done for quite some time on our behalf, because you have the ability to make the determination if it's reasonable or not.

que la Loi sur l'accès à l'information et la protection de la vie privée ne s'y applique pas.

**M. Dufresne :** Elle ne s'y appliquerait pas. Vous pouvez l'inclure en modifiant des règlements et en fournissant davantage de détails sur ce point. Il existe peut-être des possibilités, mais, encore une fois, dans le cas présent, le projet de loi prévoit ces pouvoirs et apporte cette clarté. Vous avez l'occasion de le faire dès maintenant. Je ne veux pas présumer de la date où la Loi sur l'accès à l'information et la protection de la vie privée sera modifiée, donc vous avez l'occasion de le faire.

**La sénatrice Batters :** À quand remontait la dernière fois que cette loi a été modifiée? Était-ce lors du projet de loi C-15?

**M. Dufresne :** Cela remonte à 40 ans. Peut-être que quelques petits amendements ont été apportés durant cette période, mais, assurément, quelque chose aurait dû être fait il y a longtemps.

**La sénatrice Batters :** Merci.

**Le président :** Chers collègues, il n'y a plus d'autres sénateurs qui figurent sur la liste des intervenants, donc je me permets de poser une question à M. Noël.

Vous avez un rôle important à jouer en tant que commissaire en chef au renseignement. Compte tenu de votre responsabilité d'agir en tant que gardien des valeurs et principes fondamentaux de notre démocratie et de votre responsabilité à l'égard du pouvoir d'intervention de l'État et la détermination de cet équilibre... chaque fois que vous avez comparu ici et que vous avez parlé de cet équilibre, vous l'avez fait de manière très éloquente. Dans le cas du présent projet de loi, votre rôle, votre responsabilité et votre marge de manœuvre ont été amoindris. Pourriez-vous m'expliquer pourquoi?

**M. Noël :** Je ne sais pas pourquoi les auteurs de ce projet de loi ont décidé de... je n'ai pas été consulté. On ne m'a pas tenu au courant. Cependant, il y a quelques jours de cela, ils m'ont fait une offre, que j'ai refusée, car je suis un agent indépendant. Je ne sais pas pourquoi ils ont décidé de mettre à l'écart cette surveillance.

**Le président :** Compte tenu de la responsabilité extrêmement importante de la cybersécurité pour l'ensemble de la nation, et pas seulement pour les particuliers, il demeurera toujours un équilibre à trouver dans l'intérêt du pays, en protégeant les Canadiens et les institutions dans de nombreux endroits, mais ne serait-il pas juste pour les Canadiens de vouloir comprendre que chaque fois qu'il est nécessaire de trouver un moyen de faire face à la gravité de la situation, nous aurions donc quelqu'un pour assurer une surveillance, ce que vous avez fait pendant passablement de temps en notre nom, parce que vous avez la capacité de déterminer si cela est raisonnable ou non.

**Mr. Noël:** As with the Privacy Commissioner's job, the Intelligence Commissioner's job is there to insert into the population a degree of confidence. That's why we're there. I feel like a goaltender, and it is my information. When I look at what CSE is doing, I have a view of it as if it's mine. I want to make sure that if they have to keep it, they have good reasons to do so. I want to make sure, secondly, that if they have to keep it, how long they are going to keep it. It's so important for me when I look at that type of information.

Cyberattacks are as the war of the present time. Canada is open to state attacks like it is to ransom attacks. We have to give our governments the tools to respond. You can't give them a little shotgun, they have to have the same kinds of resources.

At the same time — the balancing that you're talking about — there has to be an oversight, including a review process with the National Security and Intelligence Review Agency, or NSIRA, and the National Security and Intelligence Committee of Parliamentarians, or NSICOP in order to make sure that these important tools are properly used and that the privacy of Canadians at the end is protected. That's why we're there. That's why the Privacy Commissioner is there.

In this case, they decided to leave aside the oversight and they made a big point about having the review, but they forgot that an oversight, like the Intelligence Commissioner, is a different one. It's not the same as the review process, because the review process comes after the fact.

The Privacy Commissioner has an investigation power like NSIRA. At my stage, I deal directly with the operators. To that effect, it appears to me — and history has shown that up until now, that this job has evolved and things cannot be known now, but one day it will come out that it has been extremely useful.

**The Chair:** Thank you very much.

Colleagues, this brings us to the end of this panel. I want to thank the three witnesses who are before us today. Each one of them in their own capacity provides an important service to the country, and it is invaluable what you do on behalf of Canadians. Thank you for your service to the country. We very much appreciate the experience you bring and the insight you provide to the committee in regard to the questions we asked.

**M. Noël :** Tout comme le commissaire à la protection de la vie privée, le commissaire au renseignement a pour rôle de procurer à la population un certain degré de confiance. C'est notre raison d'être. Je me sens comme un gardien de but, et il s'agit de mes informations. Lorsque je regarde ce que fait le CST, je le perçois comme s'il m'appartenait. Je veux m'assurer que si le centre doit garder ces informations, qu'il ait de bonnes raisons de le faire. Je veux également m'assurer, dans un deuxième temps, que s'ils doivent la conserver, la durée de conservation de cette information. Cela est très important pour moi lorsque je regarde ce type d'information.

Les cyberattaques sont la guerre des temps modernes. Le Canada est vulnérable aux attaques étatiques comme il l'est aux rançongiciels. Nous devons outiller nos gouvernements pour qu'ils puissent répondre à ces dangers. Vous ne pouvez pas leur donner un petit fusil... ils doivent être en mesure de combattre le feu par le feu et disposer du même genre de ressources.

En même temps — quant à l'équilibre dont vous parlez — il doit y avoir une surveillance qui comprend un processus d'examen en collaboration avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ou OSSNR, et le Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, afin que l'on puisse s'assurer que ces outils importants sont utilisés de manière appropriée et que la vie privée des Canadiens est ultimement protégée. C'est pour ces raisons que nous existons. C'est pour cette raison que le commissaire à la protection de la vie privée existe.

Dans le cas présent, les auteurs du projet de loi ont décidé de mettre de côté l'aspect de la surveillance, et ils ont fait tout un plat du fait qu'un examen est prévu, mais ils ont oublié qu'une surveillance, comme celle qu'assure le commissaire au renseignement, est d'une nature différente. Ce n'est pas la même chose qu'un processus d'examen, car le processus d'examen survient après coup.

Le commissaire à la protection de la vie privée a un pouvoir d'enquête comme l'OSSNR. À mon palier, je travaille directement avec les exploitants. À cet égard, il semble — et l'histoire l'a prouvé jusqu'à présent — que ce travail a évolué et que les choses ne peuvent être connues aujourd'hui, mais qu'un jour on s'apercevra qu'il a été extrêmement utile.

**Le président :** Merci beaucoup.

Chers collègues, c'est ainsi que prend fin notre rencontre avec ce groupe de témoins. Je tiens à remercier les trois témoins qui ont comparu aujourd'hui. Chacun d'entre eux, dans son poste, fournit un service important au pays, et ce que vous faites au nom des Canadiens est inestimable. Je vous remercie pour les services que vous rendez à notre pays. Nous apprécions grandement les expériences et les perspectives que vous apportez au comité en ce qui concerne les questions que nous vous avons posées.

Senators, this brings us to the end of this part of today's agenda. We have one issue for the committee to consider, which is a budget for us to travel for the study of military procurement.

You should have received a copy of the proposed budget report and communication plan for travel in relation to the committee's study on military procurement and Canadian defence industry. This budget proposes funds for a one-day fact-finding mission to western Quebec in the area of Mirabel, where the committee members would meet with a small group of companies specializing in the production of defence capable assets.

Would members like to proceed in camera to discuss the budget? Agreed?

**Hon. Senators:** Agreed.

(The committee continued in camera.)

(The committee resumed in public.)

**The Chair:** It is agreed that the budget application for travel to western Quebec for a fact-finding mission for the fiscal year ending March 31, 2025, be approved for submission to the Standing Senate Committee on Internal Economy, Budgets and Administration.

All those in favour?

**Hon. Senators:** Agreed.

**The Chair:** Agreed. Thank you, senators.

This budget will now be submitted to the Standing Senate Committee on Internal Economy Budgets and Administration to be reviewed by the Subcommittee on Senate Estimates and Committee Budgets, or SEBS, at the earliest opportunity.

This concludes today's agenda. Our next meeting will take place Monday, November the 25, at 4 o'clock Eastern Time. We will proceed to clause-by-clause consideration of Bill C-26. Members are encouraged to contact the Office of the Law Clerk or parliamentary counsel should they wish to bring forward amendments and to share amendments with the clerk as soon as possible. If you would like your amendments to be distributed in advance of the meeting, please share them with the clerk by Friday morning, November 22, at the latest. Otherwise, please bring sufficient copies of your amendments to the meeting. With that, I wish everybody a good night.

(The committee adjourned.)

Chers sénateurs et chères sénatrices, nous voici rendus à la fin de l'ordre du jour d'aujourd'hui. Il reste une question dont le comité doit traiter, et il s'agit d'un budget de déplacement pour l'étude sur l'approvisionnement militaire.

Vous devriez avoir reçu une copie du rapport de budget proposé et le plan de communication pour les déplacements liés à l'étude du comité sur l'approvisionnement militaire et l'industrie de défense canadienne. Ce budget propose un financement pour une mission d'enquête d'une journée dans l'Ouest du Québec, dans la région de Mirabel, où les membres du comité rencontreront un petit groupe d'entreprises se spécialisant dans la fabrication de biens utiles pour la défense.

Les sénateurs souhaitent-ils passer à huis clos pour discuter du budget? Êtes-vous d'accord?

**Des voix :** Oui.

(La séance se poursuit à huis clos.)

(La séance publique reprend.)

**Le président :** Il est convenu que la demande de budget pour le voyage dans l'Ouest du Québec pour une mission d'enquête pour l'exercice se terminant le 31 mars 2025 soit approuvée pour être soumise au Comité permanent de la régie interne, des budgets et de l'administration.

Que tous ceux qui sont d'accord se manifestent.

**Des voix :** D'accord.

**Le président :** D'accord. Merci, mesdames et messieurs.

Ce budget va maintenant être soumis au Comité permanent de la régie interne, des budgets et de l'administration afin d'être passé en revue par le Sous-comité du budget des dépenses du Sénat et des budgets de comités, et ce, dès que possible.

Voilà qui conclut l'ordre du jour d'aujourd'hui. Notre prochaine réunion aura lieu le lundi 25 novembre, à 16 heures, heure de l'Est. Nous allons procéder à une étude article par article du projet de loi C-26. Les membres sont encouragés à communiquer avec le bureau du légiste et conseiller parlementaire s'ils souhaitent proposer des amendements et partager les amendements avec la greffière dès que possible. Si vous souhaitez que vos amendements soient distribués à l'avance pour la réunion, s'il vous plaît, transmettez-les à la greffière au plus tard le vendredi matin 22 novembre. Sinon, assurez-vous d'apporter suffisamment d'exemplaires de vos amendements à la réunion. Sur ce, je souhaite à tous et à toutes une excellente soirée.

(La séance est levée.)