

SENATE



SÉNAT

CANADA

First Session
Forty-second Parliament, 2015-16-17

*Proceedings of the Standing
Senate Committee on*

TRANSPORT AND
COMMUNICATIONS

Chair:
The Honourable DENNIS DAWSON

Tuesday, June 13, 2017
Wednesday, June 14, 2017

Issue No. 20

Twenty-third and twenty-fourth meetings:

Study on the regulatory and technical issues related to the
deployment of connected and automated vehicles

WITNESSES:
(See back cover)

Première session de la
quarante-deuxième législature, 2015-2016-2017

*Délibérations du Comité
sénatorial permanent des*

TRANSPORTS ET DES
COMMUNICATIONS

Président :
L'honorable DENNIS DAWSON

Le mardi 13 juin 2017
Le mercredi 14 juin 2017

Fascicule n° 20

Vingt-troisième et vingt-quatrième réunions :

Étude sur les questions techniques et réglementaires liées
à l'arrivée des véhicules branchés et automatisés

TÉMOINS :
(Voir à l'endos)

STANDING SENATE COMMITTEE ON
TRANSPORT AND COMMUNICATIONS

The Honourable Dennis Dawson, *Chair*

The Honourable Michael L. MacDonald, *Deputy Chair*

and

The Honourable Senators:

Beyak	Hartling
Boisvenu	Mercer
Bovey	Runciman
Cormier	Saint-Germain
Eggleton, P.C.	* Smith
Galvez	(or Martin)
Griffin	

* Harder, P.C.
(or Bellemare)

*Ex officio members
(Quorum 4)

Changes in membership of the committee:

Pursuant to rule 12-5 and to the order of the Senate of December 7, 2016, membership of the committee was amended as follows:

The Honourable Senator Bovey replaced the Honourable Senator Marwah (*June 14, 2017*).

The Honourable Senator Marwah replaced the Honourable Senator Bovey (*June 12, 2017*).

COMITÉ SÉNATORIAL PERMANENT DES
TRANSPORTS ET DES COMMUNICATIONS

Président : L'honorable Dennis Dawson

Vice-président : L'honorable Michael L. MacDonald

et

Les honorables sénateurs :

Beyak	Hartling
Boisvenu	Mercer
Bovey	Runciman
Cormier	Saint-Germain
Eggleton, C.P.	* Smith
Galvez	(ou Martin)
Griffin	

* Harder, C.P.
(ou Bellemare)

* Membres d'office
(Quorum 4)

Modifications de la composition du comité :

Conformément à l'article 12-5 du Règlement et à l'ordre adopté par le Sénat le 7 décembre 2016, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénatrice Bovey a remplacé l'honorable sénateur Marwah (*le 14 juin 2017*).

L'honorable sénateur Marwah a remplacé l'honorable sénatrice Bovey (*le 12 juin 2017*).

MINUTES OF PROCEEDINGS

OTTAWA, Tuesday, June 13, 2017
(69)

[*English*]

The Standing Senate Committee on Transport and Communications met this day at 9:30 a.m., in room 2, Victoria Building, the chair, the Honourable Dennis Dawson, presiding.

Members of the committee present: The Honourable Senators Beyak, Boisvenu, Cormier, Dawson, Eggleton, P.C., Galvez, Griffin, MacDonald, Marwah, Mercer, Runciman and Saint-Germain (12).

In attendance: Jed Chong and Nicole Sweeney, Analysts, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Wednesday, March 9, 2016, the committee continued its examination of the regulatory and technical issues related to the deployment of connected and automated vehicles. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 1.*)

WITNESSES:

Carillon Information Security Inc.:

Patrick Patterson, President.

CoinDesk:

Nolan Bauerle, Director of Research.

Ford Motor Company of Canada, Limited:

Blake Smith, Director, Sustainability, Environment and Safety Engineering.

The chair made a statement.

Mr. Patterson and Mr. Bauerle made statements and answered questions.

At 10:28 a.m., the committee suspended.

At 10:32 a.m., the committee resumed.

Mr. Smith made a statement and answered questions.

At 11:31 a.m., the committee adjourned to the call of the chair.

ATTEST:

PROCÈS-VERBAUX

OTTAWA, le mardi 13 juin 2017
(69)

[*Traduction*]

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui, à 9 h 30, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Dennis Dawson (*président*).

Membres du comité présents : Les honorables sénateurs Beyak, Boisvenu, Cormier, Dawson, Eggleton, C.P., Galvez, Griffin, MacDonald, Marwah, Mercer, Runciman et Saint-Germain (12).

Également présents : Jed Chong et Nicole Sweeney, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 9 mars 2016, le comité poursuit son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 1 des délibérations du comité.*)

TÉMOINS :

Carillon Information Security Inc. :

Patrick Patterson, président.

CoinDesk :

Nolan Bauerle, directeur de recherche.

Ford du Canada limitée :

Blake Smith, directeur en chef, Durabilité, environnement et ingénierie de la sécurité.

Le président ouvre la séance.

M. Patterson et M. Bauerle font des exposés, puis répondent aux questions.

À 10 h 28, la séance est suspendue.

À 10 h 32, la séance reprend.

M. Smith fait un exposé, puis répond aux questions.

À 11 h 31, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, Wednesday, June 14, 2017
(70)

[English]

The Standing Senate Committee on Transport and Communications met this day at 6:45 p.m., in room 2, Victoria Building, the chair, the Honourable Dennis Dawson, presiding.

Members of the committee present: The Honourable Senators Beyak, Boisvenu, Bovey, Dawson, Eggleton, P.C., Galvez, MacDonald, Runciman and Saint-Germain (9).

In attendance: Jed Chong and Nicole Sweeney, Analysts, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Wednesday, March 9, 2016, the committee continued its examination of the regulatory and technical issues related to the deployment of connected and automated vehicles. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 1.*)

WITNESS:

As an individual:

David Michelson, Co-Chair of the Intelligent Transportation Systems Society of Canada and Professor, University of British Columbia.

The chair made a statement.

Mr. Michelson made a statement and answered questions.

At 7:30 p.m., the committee suspended.

At 7:31 p.m., pursuant to rule 12-16(1)(d), the committee resumed in camera to consider a draft agenda (future business).

It was agreed that senators' staff be permitted to remain in the room while the committee met in camera.

The committee discussed a draft agenda.

At 7:36 p.m., the committee adjourned to the call of the chair.

ATTEST:

OTTAWA, le mercredi 14 juin 2017
(70)

[Traduction]

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui, à 18 h 45, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Dennis Dawson (*président*).

Membres du comité présents : Les honorables sénateurs Beyak, Boisvenu, Bovey, Dawson, Eggleton, C.P., Galvez, MacDonald, Runciman and Saint-Germain (9).

Également présents : Jed Chong and Nicole Sweeney, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 9 mars 2016, le comité poursuit son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 1 des délibérations du comité.*)

TÉMOIN :

À titre personnel :

David Michelson, coprésident, Société des systèmes de transport intelligents du Canada, et professeur, Université de la Colombie-Britannique.

Le président ouvre la séance.

M. Michelson fait un exposé, puis répond aux questions.

À 19 h 30, la séance est suspendue.

À 19 h 31, conformément à l'article 12-16(1)(d) du Règlement, la séance se poursuit à huis clos afin que le comité examine un projet d'ordre du jour (travaux futurs).

Il est convenu d'autoriser le personnel des sénateurs à demeurer dans la pièce pendant la partie de la réunion à huis clos.

Le comité discute d'un projet d'ordre du jour.

À 19 h 36, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

Le greffier du comité,

Victor Senna

Clerk of the Committee

EVIDENCE

OTTAWA, Tuesday, June 13, 2017

The Standing Senate Committee on Transport and Communications met this day, at 9:30 a.m., to continue its study on the regulatory and technical issues related to the deployment of connected and automated vehicles.

Senator Dennis Dawson (*Chair*) in the chair.

[*Translation*]

The Chair: Honourable senators, I call the meeting of the Standing Senate Committee on Transport and Communications. This morning, the committee is continuing its study on the regulatory and technical issues related to the deployment of connected and automated vehicles.

[*English*]

Today, we have two panels of witnesses. For this first panel, I would like to welcome Patrick Patterson, President of Carillon Information Security Inc.; and Nolan Bauerle, Director of Research at CoinDesk.

As you know, Mr. Bauerle, you are limited to five minutes for your presentation; you have been here often enough in the past, listening to the presentations.

Nolan Bauerle, Director of Research, CoinDesk: I have been doing some work with both the Blockchain Research Institute, Don Tapscott's outfit in Toronto, as well as CIGI, the Centre for International Governance Innovation, with the University of Waterloo and Wilfrid Laurier University, participating in round tables for governance innovation, as well as talking at conferences around the world to regulators, legislators and business people interested in this technology.

My principal work, since I began in this industry, has been with Manhattan-based CoinDesk, where I am the Director of Research. CoinDesk is the world leader in Bitcoin cryptocurrency, blockchain and distributed ledger, news and research. We host the largest and most important conference in the world related to this technology. Three weeks ago, in Times Square, we had 3,000 conference attendees, along with a full list of the brightest minds in the business, including Toyota Research Institute, who mentioned some of their announcements at our conference, at committee hearings here two weeks ago.

The most important metric of our success has been generated from our editorial team. We are the world leader in attracting eyeballs to well-written and well-scrutinized news. This team is led by Editor-in-Chief Peter Rizzo and a list of contributors too long

TÉMOIGNAGES

OTTAWA, le mardi 13 juin 2017

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui, à 9 h 30, pour poursuivre son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés.

Le sénateur Dennis Dawson (*président*) occupe le fauteuil.

[*Français*]

Le président : Honorables sénateurs et sénatrices, je déclare la séance du Comité sénatorial permanent des transports et des communications ouverte. Ce matin, le comité poursuit son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés.

[*Traduction*]

Aujourd'hui, nous allons entendre deux groupes de témoins. Permettez-moi de souhaiter la bienvenue aux deux personnes qui composent le premier, soit M. Patrick Patterson, président de Carillon Information Security Inc., et M. Nolan Bauerle, directeur de recherche chez CoinDesk.

Monsieur Bauerle, comme il vous est souvent arrivé de venir écouter ici les exposés d'autres témoins, vous savez que vous devez limiter à cinq minutes vos commentaires préliminaires. Nous vous écoutons.

Nolan Bauerle, directeur de recherche, CoinDesk : J'ai eu l'occasion de collaborer à la fois avec le Blockchain Research Institute, l'entreprise de Don Tapscott à Toronto, et avec le Centre for International Governance Innovation, le CIGI, ainsi qu'avec les universités de Waterloo et Wilfrid Laurier lorsque j'ai participé à des tables rondes sur l'innovation en gouvernance. J'ai également pris la parole lors de plusieurs conférences à travers le monde devant des responsables de la réglementation, des législateurs et des gens d'affaires intéressés par cette technologie.

Depuis que je me suis impliqué dans ce secteur d'activité, j'ai essentiellement travaillé pour CoinDesk, une société implantée à Manhattan, dont je suis le directeur de recherche. CoinDesk est le leader mondial de la cryptomonnaie bitcoin, des chaînes de blocs et des registres distribués, et de façon plus générale des nouveautés et de la recherche en la matière. Nous avons organisé la plus importante conférence dans le monde traitant de cette technologie. Il y a trois semaines, nous avons accueilli à Times Square 3 000 conférenciers, parmi lesquels une liste impressionnante des esprits les plus brillants dans ce domaine d'activité, y compris des représentants du Toyota Research Institute qui ont profité de notre conférence pour faire quelques-unes de leurs annonces, et que vous avez entendus il y a environ deux semaines.

Nous devons, dans une large mesure, notre réussite dans notre domaine de spécialisation au travail de notre équipe de rédaction. Nous sommes en effet le leader mondial pour attirer l'attention sur des nouvelles bien rédigées dont le contenu a été vérifié comme

to mention. The story we are telling is a mix of cryptography, finance, law, accounting, politics, technology and, of course, futurism.

One narrative I am interested in at CoinDesk, and something I use to help guide my research, is related to the story of cryptography. More precisely, the story of individuals wielding for themselves the full power of cryptography. Cryptography is at the heart of the problems you are studying here with the security of connected cars: how to secure communications, data and connections; how to tell secrets, maintain privacy and keep out eavesdroppers and those who would do us harm.

After World War II, the Nazi enigma machine and Alan Turing, governments realized the power of cryptography was so great that its proliferation needed to be controlled, so cryptography was counted as a gun or a munition, its commercial development severely restricted. This meant that cryptography was in the exclusive hands of the military and, for the most part, the NSA.

With the digital age, the munitions designation of cryptography ended. It was untenable, and cryptography needed to be deployed commercially in order for people to use computers.

Some of people who helped change this designation remain vital to the crypto-currency industry today; cryptographers like Adam Back, the CEO of Montreal-based Blockstream, one of the most important companies in our industry.

Cryptographic keys went from being a munition to a commercial tool, but cryptography took a detour there. In the digital world, there exists a fundamental question: Who are you? In the physical realm, this is simple. With the digital world, the answer to this question is less clear. "Who are you?" authentication became a major use case for an entire industry of cryptographic tools.

Instead of wielding private keys ourselves, users exchanged their mother's maiden name or a dog's name in exchange for these. A bank and other information providers managed our cryptographic needs for us.

il se doit. Cette équipe, composée d'un nombre de collaborateurs trop important pour pouvoir tous les citer ici, est dirigée par notre rédacteur en chef, Peter Rizzo. Les nouvelles que nous publions traitent à la fois de cryptographie, de finances, de droit, de comptabilité, de politique, de technologie, et bien sûr de la façon dont nous entrevoyons le futur.

L'un des sujets qui retiennent le plus mon attention chez CoinDesk, et auquel je me reporte parfois pour guider mes recherches, est l'histoire de la cryptographie. Plus précisément, c'est l'histoire des personnes qui, pour leur propre compte, ont cherché à saisir toute la puissance de la cryptographie, qui se révèle être au cœur des problèmes que vous étudiez ici concernant la sécurité des véhicules connectés. On doit en effet se demander comment assurer la sécurité des communications, des données et des connexions, comment échanger des secrets tout en assurant la protection des données et en se protégeant des oreilles indiscrettes et des personnes qui voudraient nous nuire?

Après la Seconde Guerre mondiale, et le décryptage par Alan Turing de la machine Enigma des nazis, les gouvernements ont pris conscience de l'utilité de la cryptographie et de la nécessité de contrôler sa prolifération. Les techniques regroupées sous ce vocable sont alors apparues comme des armes ou des munitions et les gouvernements ont fortement limité leur développement commercial. Dès lors, l'utilisation de la cryptographie a été réservée aux militaires et, pour l'essentiel, à la National Security Agency, la NSA.

L'avènement de l'ère numérique a contraint à abandonner l'assimilation de la cryptographie à des munitions. Cette approche n'était plus tenable et il devenait nécessaire de déployer ces techniques dans le domaine commercial pour permettre aux gens d'utiliser les ordinateurs.

Certaines personnes qui ont tout particulièrement contribué à faire évoluer cette approche jouent toujours un rôle essentiel dans le secteur des cryptomonnaies. On peut citer ici en particulier M. Adam Back, le PDG de la société montréalaise Blockstream, l'une des plus importantes dans notre secteur d'activité.

Les clés de chiffrement, ou cryptographiques, sont passées du statut de munitions à celui d'outils commerciaux, mais pour y parvenir, la cryptographie a dû emprunter une voie de contournement. Lors de toute transaction, au sens large, il faut en effet se poser une question fondamentale : Qui êtes-vous? On veut savoir si on échange avec la bonne entité. Dans le domaine du concret, la réponse est simple. Dans le monde numérique, la réponse à cette question est moins évidente. Cette question et la réponse à y apporter sont devenues des cas pratiques importants pour l'ensemble du secteur des outils cryptographiques.

Au lieu de s'exercer eux-mêmes à l'utilisation des clés privées, les utilisateurs échangent le nom de jeune fille de leur mère ou celui de leur chien plutôt que de telles clés. Ce sont les banques et les autres prestataires de services d'information qui gèrent pour nous nos besoins de cryptographie.

But this arrangement is under siege. So many privacy breaches you hear of — every large-scale hack — can be traced to vulnerabilities created by the mere introduction of a third party into our cryptographic authentication.

We have shared our entire lives all in exchange for authentication. Satoshi Nakamoto, the mythical creator of Bitcoin, warned that banks and service providers must be wary of their customers, as they need to collect more private information than is necessary in order to transact. The result is something akin to a public health epidemic.

How Bitcoin solved authentication was to put cryptographic keys in the hands of users and in the hands of individuals. Possession of a cryptographic key is ownership in Bitcoin. In the case of Bitcoin and other crypto-currencies, possession is ownership. This is the newest development in the story of cryptography: from a munition, to a service provided in exchange for your mother's maiden name to, finally, cryptographic keys in the hands of individuals.

The implications of this shift represent a revolution. Because keys and security are with users, Bitcoin has also spurred a major innovation in the physical security of cryptographic keys. Early adopters suddenly needed to manage their own keys, and a market for digital wallets that store and generate cryptographic keys grew. This market has led to amazing physical wallets that are excellent at privacy protection and new microchips that have trusted encryption enclaves that allow for keys to stay in a device and never expose themselves to the connections of the Internet.

Secure key management and on-device cryptographic key transactions are an important consideration for connected cars as the industry moves forward. It is this innovation, along with several others, but this one in particular, that has a role to play with connected cars.

Machines and sensors that are connected in cars are not going to be able to submit a mother's maiden name in order to be authenticated by a third party. The only way forward is to extend Bitcoin's authentication logic. The same way possession of keys means ownership of Bitcoin, the possession of cryptographic keys means authentication of machines and connected devices in cars themselves. In short, these sensors might end up looking a lot like a Bitcoin wallet.

Cette façon de procéder fait maintenant l'objet de vives critiques. Un grand nombre des atteintes à la vie privée dont vous entendez parler et tous les piratages à grande échelle ont été rendus possibles par des vulnérabilités imputables à la simple introduction d'une tierce partie dans nos modalités d'authentification cryptographique.

Pour parvenir à nous authentifier, nous n'avons d'autre choix que de partager l'intégralité de nos vies. Satoshi Nakamoto, le créateur mythique des bitcoins, nous a prévenus que les banques et les prestataires de services doivent être las de leurs clients, car ils sont tenus de recueillir plus de renseignements privés que nécessaire pour être en mesure d'exécuter des transactions. On se retrouve dans une situation qui fait penser à une épidémie dans le domaine de la santé publique.

La technologie des bitcoins a résolu ce problème d'authentification en confiant les clés cryptographiques aux utilisateurs et aux personnes. La possession d'une clé cryptographique revient à la possession de bitcoins. Dans le cas des bitcoins et des autres cryptomonnaies, la possession de la clé témoigne de la propriété de la cryptomonnaie. C'est là le développement le plus récent dans l'histoire de la cryptographie : en passant d'une munition à un service fourni en échange du nom de jeune fille de votre mère, les clés cryptographiques se trouvent enfin dans les mains des personnes.

Les implications de ce changement constituent en elles-mêmes une révolution. Les clés et la sécurité sont en effet dorénavant dans les mains des utilisateurs. L'apparition des bitcoins a également favorisé une innovation majeure dans la sécurité matérielle des clés cryptographiques. Les premières personnes à avoir adopté cette cryptomonnaie ont en effet réalisé qu'elles devaient gérer leurs propres clés, et on a alors vu se développer un marché pour les portefeuilles numériques qui entreposent et génèrent des clés cryptographiques. Ce marché a favorisé l'apparition de portefeuilles surprenants qui sont excellents pour assurer la protection des renseignements personnels, et de micro puces dotées d'un cryptage fiable qui permet de conserver les clés dans un appareil sans qu'il soit jamais possible de les exposer à une connexion Internet.

Alors que l'industrie progresse dans le domaine des voitures connectées, la gestion sécuritaire des clés et les transactions de clés cryptographiques résidant sur un dispositif constituent des atouts importants pour ces véhicules. Même s'il y a plusieurs autres innovations intéressantes dans ce domaine, c'est précisément celle-ci qui a un rôle majeur à jouer dans le cas des voitures connectées.

Les appareils et les capteurs connectés dans les voitures ne pourront pas communiquer le nom de jeune fille de la mère pour être authentifiés par une tierce partie. La seule solution pour l'avenir est d'appliquer à plus grande échelle la logique utilisée pour l'authentification des bitcoins. Tout comme la possession des clés atteste de la propriété des bitcoins, la possession des clés cryptographiques constituera en soit l'authentification des appareils et des dispositifs connectés dans les voitures elles-mêmes. En résumé, ces capteurs pourraient bien finir par ressembler passablement à un portefeuille de bitcoins.

Blockchain technology and Bitcoin achieve something called privacy by design and, because of this, it is compliant with privacy laws. Keys remain with the users and there is no need to force other parties to share too much data, limiting the surface area of attack for those who would do us harm. Thank you.

Patrick Patterson, President, Carillon Information Security Inc.:
Good morning. I would like to thank the committee for the opportunity to speak with you regarding the importance of cyber security in the context of autonomous and connected vehicles. I work for Carillon Information Security Inc., a firm based in the Montreal area that has been involved in the standardization of identity management policies for the aerospace and U.S. government areas for the last 16 years.

We have been intimately involved in the entire history of e-enabled aircraft. We already have autonomous and connected vehicles. They are flying over our heads right now.

We faced many of the same challenges as you are looking at today in the context of autonomous cars and other kinds of vehicles, but I would also challenge that we should broaden it and take a look at things like autonomous naval ships and, again, aircraft, trains and other things, because they are all beginning to do exactly the same thing. They are all beginning to send and receive digital information and get their signalling information completely digitally. We are beginning to do things like transmit software from a manufacturer down to a vehicle. I will not talk about cars, but just generic vehicles, because we are doing it in just about every single sector right now.

As Mr. Bauerle said, identity is the key to cyber security. If we don't know who we are talking to, we have no idea whether we should trust them and listen to the message they are sending or unpack that piece of software they are sending us.

The other piece is integrity. We need to ensure that that piece of software that left the manufacturer or that message that left the signalling centre actually gets to the correct vehicle and is also decoded and able to be trusted as not having been tampered with in transit.

As I said, some of the applicability areas include software updates. We have been intimately involved in the security of software updates to aircraft. Now we are looking around to the field of autonomous cars, and even semi-autonomous cars: take a look at companies like Tesla, which is already beaming software directly to your car. If you have a Tesla and you walk in in the

La technologie des chaînes de blocs et des bitcoins a abouti à ce qu'on appelle la « protection de la vie privée dès la conception ». De par sa nature même, celle-ci est conforme aux exigences de la législation sur la protection des renseignements personnels. Ce sont les utilisateurs qui conservent les clés cryptographiques et il n'est pas nécessaire d'exiger de tierces parties qu'elles partagent une trop grande quantité de données. Cela réduit l'étendue des domaines susceptibles de faire l'objet d'attaques par des personnes voulant nous nuire. Je vous remercie.

Patrick Patterson, président, Carillon Information Security Inc. :
Bonjour, mesdames et messieurs. Je tiens à remercier les membres de votre comité de me fournir ainsi l'occasion de m'adresser à vous pour aborder l'importance de la cybersécurité dans le cas des véhicules autonomes et connectés. Je suis au service de Carillon Information Security Inc., une société montréalaise qui œuvre depuis 16 ans dans le domaine de la normalisation des politiques de gestion de l'identité pour le secteur de l'aérospatiale et pour le gouvernement des États-Unis.

Nous avons été impliqués très étroitement dans toute la chronologie ayant abouti à ce qu'on appelle les avions informatisés. Nous disposons déjà de véhicules autonomes et connectés. Ils volent actuellement au-dessus de nos têtes.

Nous sommes confrontés dans une large mesure aux mêmes défis qui se posent aujourd'hui aux voitures et aux autres types de véhicules autonomes. Je suis convaincu que nous devrions élargir la question et nous pencher sur divers sujets connexes comme, outre les avions, les navires, les trains et d'autres moyens de transport autonomes parce qu'ils commencent tous à fonctionner de la même façon. Ils commencent tous à envoyer et recevoir des données numériques et à récupérer les informations concernant leur signalisation de façon complètement numérique. Nous commençons à faire des choses comme transmettre des logiciels d'un fabricant vers un véhicule. Je ne vais pas vous parler des voitures, mais plutôt de véhicules génériques, parce que nous sommes confrontés actuellement aux mêmes problèmes dans pratiquement tous les secteurs du domaine des transports.

Comme M. Bauerle vous l'a rappelé, la clé de la cybersécurité est l'identité. Si nous ignorons à qui ou à quoi nous parlons, nous ignorons également si nous devrions faire confiance à cette personne ou à ce système et écouter les messages qu'il ou elle nous adresse ou utiliser le logiciel qu'il ou elle nous envoie.

L'autre élément important est l'intégrité de la transmission. Nous devons nous assurer que le logiciel parti du fabricant ou le message adressé par le centre de signalisation parvient au bon véhicule, qu'il a été décodé comme il convient et que nous pouvons lui faire confiance en ayant la conviction qu'il n'a pas été altéré pendant la communication.

Comme je l'ai déjà dit, parmi les domaines dans lesquels ces préoccupations s'appliquent, on peut citer la mise à jour des logiciels. Nous avons été étroitement impliqués dans la sécurité des mises à jour de logiciels à bord des avions. Maintenant, si nous élargissons la question en nous intéressant au domaine des voitures autonomes, et même des voitures semi-autonomes :

morning, you have a button that says, “Hi, you received a software update overnight,” a bit like your Windows system, which is kind of scary.

We are doing that today with enabled aircraft. We can take a piece of software that leaves a manufacturer — whoever writes that software goes to the OEM, whoever is producing that aircraft, which then gets transmitted out to the operator and they will then beam it to their aircraft. Once it gets on the aircraft, a technician can come on board, hit a button, watch the light go green — hopefully — and know that that piece of software is exactly the same and is coming from a trusted source as the one that originated and went through all of the various QA steps along the chain of custody.

The other one is communications with trusted sources. When we are talking about trains, ships, airplanes and sometimes about cars, these vehicles will be receiving signals from various points of infrastructure along the way. Some are already happening today in an unauthenticated fashion. In the aerospace industry, this is becoming increasingly important, because we are moving away from voice communications to pure data. A pilot will no longer hear an air traffic controller on the other end of the line; they will get a message that says, “Hi, aircraft ABC. Climb to 10,000 feet at heading 2-1-3.” They have to be able to know that the message absolutely came from an air traffic control centre. Trains and ships will each get the same thing.

For cars, it will be a bit different. It might be a message from the roadside saying, “Hi. Your maximum speed limit in this sector is not 90 as the GPS would tell you; rather, it’s 70 because of road work” or some other event going on. We still need to be able to authenticate the sources of those messages.

Then there is the inter-vehicle communication. The way a lot of this autonomous technology works is that you have a car sitting there going, “Hi. I am here. I am going this fast at this particular heading” and people or vehicles around you know exactly what is going on.

With the ADSB system with aircraft, that is where they are moving to as well. An aircraft, instead of having a radar vector, they have collision avoidance systems and also the ADSB systems where the aircraft is saying, “Hi. I’m at 30,000 feet over this point of ground, going in this direction at this speed.”

voyons comment les choses se passent dans des entreprises comme Tesla, qui transmet déjà directement des logiciels vers votre voiture. Si vous êtes propriétaire d’une voiture de cette marque, lorsque vous montez dans celle-ci le matin, un message peut s’afficher vous disant : « Bonjour. Vous avez reçu cette nuit une mise à jour du logiciel. » C’est un peu comme avec le système Windows, et cela peut vous inquiéter.

C’est ce que nous faisons aujourd’hui avec les avions informatisés. Nous pouvons prendre un logiciel qui provient du fabricant, ou de qui que ce soit qui a écrit ce logiciel et l’a transmis au fabricant d’équipement d’origine, qui que soit le fabricant de cet avion, qui est ensuite transmis à son exploitant qui va lui-même le télécharger à bord de son avion. Une fois cela fait, un technicien peut monter à bord, appuyer sur un bouton et voir le témoin virer au vert, du moins on l’espère, et avoir alors la certitude que ce logiciel n’a pas été trafiqué et provient d’une source fiable, comme celle de la version originale qui a franchi toutes les étapes d’assurance de la qualité de la chaîne de contrôle.

L’autre élément important est de s’assurer que les communications se font avec des sources fiables. Lorsque nous parlons de trains, de navires, d’avions et parfois de voiture, ces véhicules recevront des signaux de divers éléments d’infrastructure le long de leur route. Cela se produit d’ailleurs dès aujourd’hui dans certains cas sans authentification. C’est un phénomène qui ne cesse de s’étendre dans le secteur de l’aérospatiale parce que nous abandonnons les communications vocales en les remplaçant par des transmissions de données. Un pilote n’aura bientôt plus à écouter un contrôleur de la circulation aérienne s’adressant à lui; il recevra un message qui dit : « Bonjour, avion ABC, grimper à 10 000 pieds et mettez le cap aux 2-1-3. » Il faudra alors qu’il ait la certitude absolue que le message provient bien d’un centre de contrôle de la circulation aérienne. Il en ira de même pour les trains et les navires.

La situation sera un peu différente dans le cas des voitures. Il se peut en effet que vous receviez des messages provenant d’équipements en bordure de la route et vous disant : « Bonjour, la vitesse maximale autorisée dans ce secteur n’est pas de 90 km/h comme votre GPS vous l’indique, mais plutôt de 70 km/h parce que des travaux y sont en cours. » Un tel système pourra également vous prévenir de n’importe quel autre type de danger ou vous transmettre des instructions précises. Là aussi, il faudra être en mesure d’authentifier l’origine de ces messages.

Viennent ensuite les problèmes de communications entre véhicules. Quantité de technologies assurant l’autonomie d’un véhicule ont besoin que votre voiture prévienne les autres en leur disant « Je suis ici. Je roule à la vitesse de tant de km/h dans cette direction. » Les personnes ou les véhicules se trouvant proches de vous sauront alors exactement ce qui se passe.

Maintenant que les avions sont équipés de systèmes de surveillance dépendante automatique en mode diffusion, ou ADS-B, l’avion, au lieu d’être représenté sous forme d’un vecteur sur un écran radar, dispose de son propre système d’évitement des collisions. Le système ADS-B, lui, va émettre un message disant : « Je vole au cap XXX à 30 000 pieds au-dessus du point YYY à la vitesse de ZZZ km/h. »

All of these things are exactly the same problem, so we need to take a look at it in a completely holistic manner. We can't take a look at it as Transport Canada makes one set of rules for airplanes, another for trains, another for ships and another for cars. This will work best if it is a common set of standards or at least a common set of principles.

In the aerospace industry, there is already a bunch of ways of doing this — of standards that have been created. We have worked over the last 16 years to go through and standardize each of these individual sectors. We have worked with ICAO, IATA, FAH, Transport Canada, IASA — all of the worldwide regulators — so that when you have a C Series aircraft made here in Canada by Bombardier, an Airbus aircraft or a Boeing aircraft, all of them use exactly the same mechanisms and methodology.

That allows you to solve the cross-border or cross-national problem. If we take a look at this as a single insular Canadian issue, that's not going to work. We will have to take a look at this in the context of a broad global context. Manufacturers will not want to make a car that is only for Canada, just like an aerospace manufacturer doesn't make an airplane that is only for Canada. We want to have something that is truly across borders and is exactly right.

The other thing we really need to encourage Transport Canada to do is not to issue broad directives. They need to issue specific guidance. We've seen this over the last 16 years in the aerospace industry, where they issue us broad things like "you should take into account the cybersecurity considerations for doing X," which is great — thank you for making us think about it — but it doesn't help solve the problem, and it doesn't help solve it in a standard way. They need to say, "We need to solve it. You need to take this into accounts and apply X, Y and Z" — very specific standards in order to make it work.

Thank you very much.

The Chair: Thank you, Mr. Patterson. We will begin questions.

Senator Runciman: Thank you, gentlemen. You talked about specific standards versus broad guidelines. You were relating it with respect to the privacy issues and cybersecurity. I would like to get more explanation from Mr. Bauerle about cryptography, because I wasn't quite clear in the application to the issue we are studying. Maybe you can be a bit more down-to-earth, if you will,

Tous ces exemples posent exactement le même problème. Il faut donc que nous l'abordions d'une façon complètement holistique. Il ne suffit pas que Transports Canada énonce un ensemble de règles pour les avions, un autre pour les trains, un autre pour les navires et un autre pour les voitures. Nous obtiendrons de meilleurs résultats si nous disposons d'un ensemble commun de normes ou au moins d'un ensemble commun de principes.

Dans le secteur aérospatial, on dispose déjà de toute une série de façons de faire cela, d'utiliser des normes qui ont été élaborées à cette fin. Cela fait maintenant 16 ans que nous travaillons sur ces questions et nous nous efforçons de normaliser chacun de ces secteurs particuliers. Nous avons collaboré avec l'AISA, la FAA, l'IATA, l'OACI, Transports Canada, ou si vous préférez avec tous les responsables de la réglementation dans le monde, afin que lorsque vous avez un avion de la C Series fabriqué ici, au Canada, par Bombardier ou un avion Airbus ou encore Boeing, tous utilisent le même mécanisme et la même méthodologie.

Cela vous permet de résoudre les problèmes qui se posent en franchissant la frontière ou en passant d'un pays à l'autre. Si nous les abordons en adoptant un point de vue canadien « isolationniste », nous n'irons nulle part. Pour réussir, nous n'aurons d'autre choix que de nous placer dans le contexte mondial. Les fabricants d'automobiles ne seront pas intéressés à fabriquer des voitures destinées uniquement au Canada, pas plus que les fabricants d'avions ne fabriqueront des avions ne pouvant voler que sur notre territoire. Nous allons vouloir disposer de systèmes vraiment utilisables au-delà de nos frontières.

Nous devons également tout faire pour inciter Transports Canada à ne pas émettre de directives à large portée. Ces directives doivent être consacrées à des sujets précis. C'est une situation que nous avons vécue au cours des 16 dernières années dans le secteur de l'aérospatiale, alors que ses directives comportaient couramment des énoncés comme : « Dans ce domaine, vous devriez tenir compte des considérations en matière de cybersécurité. » C'est très bien en ce sens que cela nous amène à y penser, mais cela n'aide en rien à résoudre le problème ni à y apporter une solution normalisée. Les directives du ministère devraient plutôt dire : « Nous devons résoudre ce problème. Pour cela, nous allons devoir tenir compte de tel et tel élément et appliquer les mesures X, Y et Z. » Nous avons besoin de normes très précises que nos solutions devront respecter.

Je vous remercie de votre attention.

Le président : Je vous remercie, monsieur Patterson. Nous allons maintenant passer à la période de questions et de réponses.

Le sénateur Runciman : Merci à vous deux, messieurs. Au sujet des questions de protection des renseignements personnels et de la cybersécurité, vous nous avez dit souhaiter l'adoption de normes précises au lieu de nous en remettre à des lignes directrices à large portée. J'aimerais demander à M. Bauerle de plus amples détails sur la cryptographie parce que je ne suis pas sûr d'avoir

in terms of folks who aren't in that kind of field to better understand the implications and what recommendations you might be making for us as a committee to provide the government.

I am interested in the hacking vulnerability of automated vehicles. Could you speak about the potential vulnerability to cyberhacks by unauthorized third parties and how we can come to grip was that particular issue?

Mr. Bauerle: The first question was on standards and the second on vulnerabilities.

Senator Runciman: Yes.

Mr. Bauerle: With cars communicating between each other, they use the 5.9 gigahertz range. You heard Toyota research mention quite a bit about that and how this particular piece of spectrum is under siege in America. It's making sure this piece of radio frequency remains dedicated to cars.

The standards that we have developed for this imply necessarily that a third party will manage cryptographic authentication and that the government itself becomes the administrator of a root key. They are in the middle of that. They gather the data to authenticate these machines, whether there are sensors in the devices or not.

The very idea that bitcoin eliminated banks as third parties — what they really meant was that they eliminated banks as the third party for the cryptography needed to exchange. That same logic applies to cars. One of the ideas I am hoping this committee will pass on is that the government doesn't always insist on being a certificate authority, because the mere introduction of a third party into authentication creates the vulnerability itself. The very idea that we have asked another entity to authenticate us has created the surface area that is used to hack the cars.

The FBI, for example, came out with its list of white-hat hackers. They work for universities or organizations, and they try to test these devices to their limits. The telematics we have in cars these days for insurance purposes is a connected device. They will give you a lower premium, in theory, if they see your braking and speed habits. But the problem was that these devices themselves allowed cars to be targeted on the street. Now we know who that is. This insurance company that just wants to be an insurance company has had to, all of a sudden, develop cryptographic techniques as important as a bank. They have had to develop cutting-edge cryptographic technologies. Cryptography is a rare field. It is easy to propose solutions that work but it relies on its antithesis; it relies on people hacking it and breaking it in order for us to ensure it works.

très bien saisi l'intérêt de cette question pour le sujet que nous étudions. Peut-être pourriez-vous nous fournir des détails un peu plus concrets pour nous permettre, alors que nous ne sommes pas des spécialistes en la matière, de mieux comprendre les répercussions de cette technologie et de mieux appréhender les recommandations que vous souhaitez que notre comité transmette au gouvernement.

La vulnérabilité au piratage des véhicules autonomes est une question qui m'intéresse. Pourriez-vous nous parler de leur vulnérabilité éventuelle au piratage informatique par des tierces parties non autorisées et nous expliquer comment nous devrions nous y prendre pour faire face à ce risque précis.

M. Bauerle : La première question portait sur les normes et la seconde sur les vulnérabilités.

Le sénateur Runciman : C'est bien ça.

M. Bauerle : Lorsque les voitures communiquent entre elles, elles le font dans la bande des 5,9 GHz. Les représentants du Toyota Research Institute vous en ont parlé en détail en vous précisant que quantité d'autres utilisateurs voudraient, en Amérique, pouvoir utiliser cette partie du spectre des radiofréquences. Il faut donc s'assurer que l'utilisation de la bande des 5,9 GHz reste réservée aux voitures.

Les normes que nous avons élaborées en la matière supposent qu'une tierce partie gère l'authentification cryptographique et que le gouvernement lui-même devienne l'administrateur de la clé racine. Il se trouve au cœur du problème. Il recueille les données pour identifier ces machines, qu'il s'agisse ou non de détecteurs implantés dans les équipements.

L'affirmation voulant que le bitcoin élimine le recours aux banques comme tierces parties signifie en réalité que cette cryptomonnaie élimine le besoin de tierces parties pour assurer la cryptographie permettant de procéder aux échanges. La même logique s'applique aux voitures. L'une des idées que j'espère que ce comité transmettra au gouvernement est qu'il ne faudrait pas qu'il tienne dans tous les cas à être le responsable de la certification parce que la simple introduction d'une tierce partie dans le processus d'authentification fait apparaître la possibilité du piratage des voitures.

C'est ainsi que le FBI a publié une liste de « chapeaux blancs ». Ce sont des personnes au service d'universités ou d'autres organismes qui essaient de tester ces équipements jusqu'à leurs limites. C'est à des fins d'assurance que la télématique embarquée actuellement dans nos voitures prend la forme d'équipements connectés. En théorie, votre compagnie d'assurance va réduire le montant de votre prime si elle observe que vous freinez à temps et que vous n'avez pas l'habitude de dépasser la vitesse permise. Le problème est par contre que ces équipements permettent de cibler les voitures qui se trouvent sur la route. Nous savons maintenant qui en est responsable. Cette compagnie d'assurance qui ne s'intéressait qu'à l'assurance a dû, tout d'un coup, se doter de techniques cryptographiques aussi importantes que celles utilisées par les banques. Elle a dû adopter des processus à la toute pointe de

One of the interesting things about bitcoin is that by eliminating third-party authentication, it spends literally zero dollars securing the network, yet it has never been hacked. It has a feature called anti-fragility. You can think of traditional cybersecurity and cryptographic security as an onion. You pack more layers of security onto that, but you still centralize the information. It is still in one place, which makes it a target.

It only requires one weakness. It is not a fair fight between hackers and cryptographers trying to secure your information. You can devise a beautiful system that looks great on paper, but with one little weakness, hackers get in and get it all.

Bitcoin distributed this around a large area so that attacks come into the network, and it gets stronger as it's attacked. The more people that attack bitcoin, the stronger it becomes, which is different from what we have used all these years in cryptographic authentication.

My message, and this is what I hope the committee will ponder and have other departments ponder, is that the reflex for a government to be a certificate authority — the reflex — should be questioned. I'm not saying in this instance it should be a different case. This is for testing and all kinds of development to figure out. But the idea is that these communications can be done between two machines, just like bitcoin exchanges are done between two people without anyone else involved; there is no bank, no one looking at the secure communication between these cryptographic keys; there is no appealing to a third party.

Senator Runciman: I am a bit concerned about that analogy because, in using bitcoin as an example, with vehicles we're talking about public safety and potential use for terrorism, those kinds of issues where I think my perspective on this is that government has to play a more intensive role and a more involved role with respect to automated vehicles.

Mr. Bauerle: My comment to that is if they are involved in authentication, the mere introduction and insistence on a role in the secure lines of communication open up an attack vector. Because bitcoin has put this onus on bitcoin holders to control their own keys, to be in possession and control of their own keys, it spurred a wonderful industry on its own that so far is only

la technologie en la matière. La cryptographie est un domaine encore peu répandu. Il est facile de proposer des solutions qui fonctionnent, mais on ne peut vérifier leur validité qu'en recourant à leur antithèse, soit en s'assurant que les pirates informatiques ne parviennent pas à pénétrer le système. Cela n'est ni évident ni facile et n'offre pas de garantie absolue.

L'un des volets intéressants du fonctionnement des bitcoins est qu'il élimine l'authentification par des tierces parties. Ce processus n'implique absolument aucun coût pour sécuriser le réseau et il n'a encore jamais été piraté. Il est doté d'un mécanisme qui combat sa propre fragilité. Vous pouvez visualiser la cybersécurité traditionnelle et la sécurité cryptographique comme des couches d'un oignon. Vous pouvez ajouter des couches de sécurité, mais l'information est toujours centralisée. Elle se trouve toujours à un endroit précis, ce qui en fait une cible.

Il suffit d'un seul point faible. Les pirates informatiques et les cryptographies ne se battent pas à armes égales pour assurer la sécurité de votre information. Vous pouvez concevoir un système magnifique qui semble presque parfait sur papier, mais il suffit qu'il y ait un seul petit point faible pour que les pirates parviennent à y pénétrer et à s'accaparer toute l'information qui s'y trouve.

La technologie du bitcoin répartit ce risque sur une grande surface de façon à ce que les attaques contre le réseau n'aient pour effet que de le rendre plus résistant. Plus de gens s'y attaquent et plus il devient résistant à de telles attaques. C'est un phénomène bien différent de celui auquel nous nous étions habitués pendant toutes ces années dans le domaine de l'authentification cryptographique.

Le message que je veux vous transmettre, et auquel j'espère que vous et les autres ministères allez réfléchir, est qu'il y a lieu de s'interroger sur le réflexe d'un gouvernement de tenir à être le responsable en matière de certification. Je ne dis pas nécessairement que, dans ce cas précis, il faudrait retenir une autre solution. C'est une idée qui mérite d'être mise à l'essai et appliquée à toutes sortes de développements. Au fond, on sait maintenant que ces communications sécurisées peuvent se faire entre deux machines, tout comme les échanges de bitcoins qui se font entre deux personnes sans que qui que ce soit d'autre soit impliqué. Aucune banque n'intervient, personne n'a accès aux communications sécurisées entre ces deux clés cryptographiques. Il n'y a aucune raison de faire appel à une tierce partie.

Le sénateur Runciman : Je suis un peu préoccupé par l'analogie que vous faites avec les bitcoins. Dans le cas des véhicules autonomes, nous parlons de sécurité publique et d'utilisation éventuelle à des fins terroristes. Ce sont donc là des questions dans lesquelles, à mes yeux, le gouvernement n'a d'autre choix que de s'impliquer sérieusement.

Mr. Bauerle : Ce que je peux vous dire est que si le gouvernement est impliqué dans l'authentification, le simple fait qu'il s'insère avec insistance dans les lignes sécurisées de communication revient à ouvrir un vecteur permettant les attaques. Comme avec la technologie des bitcoins, il appartient à leurs détenteurs de contrôler la sécurité de leurs propres clés. Cela a favorisé

connected theoretically to connected cars. There are start-ups working on this. There are start-ups that work with Lockheed Martin, for example.

Senator Runciman: Because of time limitations, could Mr. Patterson briefly respond to that? Do you share that view?

Mr. Patterson: I take a bit of a different view on it. I fully agree that insistence on the government necessarily always being in the loop is not necessarily a good thing. Within the aerospace industry, there is its own authentication and identity management framework that the industry has adopted and that they've made sure is compatible and trustable by the various governments that have signed on to the same identity management regime. However, they let the industry have their own authentication and issuance capability and integrity protection mechanisms.

I will disagree with Mr. Bauerle. I think that PKI certainly has a role at least in part of the equation. He and I can perhaps have a debate later with regard to whether it works for vehicle to vehicle or not. But categorically, I would say have the government make the regulations but let industry have the infrastructure that is issuing and managing keys in the vast majority of cases.

With regard to the hacking question, senator, the issue there comes down to architecture. That is, which systems are we tying together? There is a wonderful press article that came out about a year and a half ago, and I think it was Jeep, that someone figured out by broadcasting a digital FM signal to them, they could actually jump from the radio on to the command bus of the car. Now, if we ever designed that in an airplane, the engineer who did it would probably be lynched, and the regulator certainly wouldn't allow it. The idea of having a complete bidirectional link between the infotainment systems in the car and the on-board command and control system is where Transport Canada has to say no to the automotive manufacturers and anyone else who is making those things and that you have completely separate networks.

Yes, I realize you need to get speed information there so your GPS makes sense, but there has to be way that we can architect that the same way as we get information that displays on your in-flight entertainment systems about where the airplane is and how high we're flying. That comes from the cockpit, but that link is very narrow and highly protected so you can't go back through it.

l'apparition d'un secteur d'activité qui s'est développé par lui-même et qui, jusqu'à maintenant, n'est relié que de façon théorique aux voitures connectées. Des entreprises en démarrage se sont attelées à cette tâche et il y en a, par exemple, qui collaborent en ce sens avec Lockheed Martin.

Le sénateur Runciman : Comme nous ne disposons que de peu de temps, auriez-vous la bonté, monsieur Patterson, de réagir brièvement à cet énoncé? Êtes-vous du même avis?

M. Patterson : Pour moi, je vois les choses un peu différemment. Je conviens tout à fait que l'insistance du gouvernement à être toujours impliqué dans ces processus n'est pas nécessairement une bonne chose. Au sein du secteur aérospatial, les entreprises ont adopté leur propre cadre de gestion des authentifications et des identités en veillant à ce qu'il soit fiable et compatible avec les normes des divers gouvernements qui ont adhéré au même régime de gestion des identités. Ces gouvernements laissent toutefois l'industrie mettre en place ses propres moyens d'authentification et d'émission des clés et ses propres mécanismes de protection de l'intégrité.

Par contre, en ce qui concerne l'infrastructure à clés publiques, l'ICP, je ne partage pas l'avis de M. Bauerle, car je pense qu'elle a un rôle à jouer, au moins dans une partie de l'équation. Lui et moi pourrions peut-être débattre plus tard pour déterminer si cela fonctionne ou non pour les communications de véhicule à véhicule. Cela dit, j'affirme de façon catégorique que le rôle du gouvernement est de produire la réglementation, mais qu'il doit laisser l'industrie s'occuper des infrastructures qui émettent et gèrent les clés dans la vaste majorité des cas.

Quant à la question du piratage, elle nous ramène, monsieur le sénateur, à l'architecture retenue. Il faut donc savoir quels sont les systèmes que nous relient les uns aux autres. Un article excellent sur cette question a été publié il y a environ un an et demi. Si je me souviens bien, cela concernait Jeep. Quelqu'un s'est aperçu qu'en transmettant un signal numérique en modulation de fréquence à un véhicule de la marque, il pouvait en fait, en passant par la radio, accéder aux commandes du véhicule. Maintenant, tout ingénieur qui concevrait un tel système destiné à un avion se verrait probablement lynché, et il est certain que l'organisme de réglementation n'en autoriserait pas l'utilisation. C'est à Transport Canada qu'il incombe de décider s'il est tolérable qu'il y ait des communications bidirectionnelles complètes entre les systèmes d'infotainment d'un véhicule et le système embarqué de commande et de contrôle ou si ceux-ci doivent emprunter des réseaux complètement distincts. La décision ne doit en aucun cas relever du fabricant d'automobiles ou de quiconque fabricant de tels systèmes.

Je sais fort bien que vous voulez disposer de l'information sur la vitesse de votre véhicule pour pouvoir exploiter les capacités de votre GPS. Il doit toutefois y avoir une façon de concevoir cette architecture comme on le fait à bord d'un avion lorsqu'on affiche sur le système d'infotainment la position et l'altitude de l'avion. Les données proviennent du cockpit, mais passent par un canal très étroit et hautement protégé qu'il est impossible d'utiliser à rebours.

We need to ensure that we basically have two different sets of streams. On aircraft, there are actually three. There is the cockpit network, the cabin network, which is used by the flight crew, and the passenger network, and none of the three talks to each other. There is no way to get from one to the other. Autonomous cars need to have the architecture built that way.

Senator Eggleton: Picking up on your remarks, government needs to be involved when it comes to issues of safety, security and privacy. We're trying to sort out exactly where we draw the lines on those so as to not impede the attempts to advance technology but bear those basic requirements in mind.

You have talked a fair bit about bitcoin, but bitcoin is relevant to the blockchain technology. Tell me in simple terms where you see, with respect to the advancement in automotive vehicles, the benefits and the challenges to be met in terms of the use of blockchain technology. What are the pluses and minuses?

Mr. Bauerle: First, decentralization. Bitcoin and blockchain technology are an elegant solution to two challenges in the digital world. The first one I mentioned in my opening remarks: Who are you? We have to know that; authentication. Possession of a key in bitcoin becomes who you are. You own that bitcoin because you hold the key. Just like a device with a key attached to it, with keys being transacted within the device itself that never leave the device are able to authenticate that way.

Senator Eggleton: Better personal security.

Mr. Bauerle: Better personal security.

The second question is, can you do what you're trying to do? Who are you and can you do what you're trying to do? That's the area where the government can come into play. Bitcoin, doing what you're trying to do, is simple. It is exchanging a small piece of digital properties. It's the first time this ever was done and it does that very well. It is very simple. But the rules and parameters around what type of transaction can be made through blockchain technology and new advancements can be much more complex, but it remains an elegant solution to those two questions: Who are you and can you do what you're trying to do? Authentication and authorization.

Within blockchain technology, the government has a great role to play in setting the parameters of what a valid transaction is for a particular network. That is definitely a role they play.

Au fond, il faut que nous veillions à avoir des flux de données distincts. À bord des avions, il y en a trois en vérité. Il y a le réseau du cockpit, celui de la cabine, qui est utilisé par l'équipage, et le réseau des passagers. Aucun de ces trois réseaux ne permet d'échanger des données avec l'un des deux autres. Il est même impossible de passer de l'un à l'autre. Il faut que l'architecture des voitures autonomes soit conçue de cette façon.

Le sénateur Eggleton : Pour en revenir à vos commentaires, il faut donc que le gouvernement soit impliqué dans les questions de sécurité, de sûreté et de protection des renseignements personnels. Nous essayons de préciser à quel niveau il faut tirer la ligne sur ces questions afin de ne pas nuire aux tentatives d'avancement de la technologie tout en gardant à l'esprit ces exigences de base.

Vous nous avez passablement parlé des bitcoins, mais c'est un exemple pertinent quand on parle de la technologie des chaînes de blocs. Pouvez-vous me dire en termes simples, dans le cas des progrès sur les véhicules automobiles, quels sont les avantages imputables à l'utilisation de la technologie des chaînes de blocs et quels sont les défis auxquels il faut s'attendre en la matière. En d'autres termes, quels en sont les avantages et les inconvénients?

M. Bauerle : Tout d'abord, la décentralisation. La technologie des bitcoins et des chaînes de blocs est une solution élégante à deux difficultés auxquelles on fait face dans le monde numérique. J'ai déjà fait état de la première dans mes remarques préliminaires : Qui êtes-vous? Nous devons connaître la réponse à cette question. C'est l'authentification. Dans l'univers des bitcoins, c'est la possession d'une clé qui vous définit. Vous avez ce bitcoin parce que vous avez la clé correspondante. C'est comme si la clé était attachée à un appareil et la clé fera l'objet de transactions à l'intérieur de l'appareil lui-même sans jamais quitter celui-ci. C'est ainsi que vous êtes identifié.

Le sénateur Eggleton : On a donc une sécurité personnelle améliorée.

M. Bauerle : C'est exactement ça.

La seconde question qui se pose est de savoir si vous êtes autorisé à faire ce que vous voulez faire. Nous avons donc deux questions : « Qui êtes-vous? », et « Êtes-vous autorisé à faire ce que vous voulez faire? ». C'est dans ce domaine que le gouvernement peut intervenir. Dans l'univers des bitcoins, savoir si vous êtes autorisé à faire ce que vous voulez faire est simple. Il suffit d'échanger un petit élément de données numériques. C'est la première fois qu'on a procédé de cette façon et cela fonctionne très bien. C'est parfaitement simple. Par contre, les règles et les paramètres concernant les types de transactions qu'il est possible de faire en recourant à la technologie des chaînes de blocs et à d'autres nouveaux développements peuvent se révéler beaucoup plus complexes. Cela reste toutefois une solution élégante à ces deux questions : « Qui êtes-vous? », et « Êtes-vous autorisé à faire ce que vous voulez faire? ». On parle donc ici d'authentification et d'autorisation.

Dans l'utilisation de la technologie des chaînes de blocs, le gouvernement a un rôle important à jouer en définissant les paramètres de ce qui constitue une transaction valide pour un réseau donné. C'est définitivement un rôle qui lui incombe.

Senator Eggleton: Cybersecurity?

Mr. Bauerle: Yes.

Senator Eggleton: So it's much more capable of preventing a cyberattack?

Mr. Bauerle: It is this law of nature argument. Sometimes things that are simpler are better. In this case, the simplicity of bitcoin — and I understand it sounds complicated — if you see it from 35,000 feet and you compare it to traditional cryptographic architecture, it can look quite unruly, huge, like a circus big tent with all kinds of directions and keys going everywhere, like when you want to buy something on the Internet. If it's a one-click purchase, if you actually pull back and see what's behind there, there's a whole tangle and mess of stuff going on.

Senator Eggleton: But is that also a vulnerability?

Mr. Bauerle: It certainly is. Bitcoin ends up looking a lot like a vending machine. You just send the money. This is why bitcoin is so important for transactions in plastic, for example, cash versus plastic. Plastic is a pull transaction. You're basically allowing a bank to go into your wallet, take the money out and open up someone else's wallet and put it in. In the case of bitcoin, it's exactly like cash. Here's the money; transaction over. That's it.

Senator Eggleton: What other challenges are there? Is there a heavy cost? Is the automotive industry likely to get into this?

Mr. Bauerle: There are several companies that are working on it already. There is a company that started in the Internet of things called Filament. They realized immediately that devices that transact with keys on them didn't exist when they came into the industry. They developed something called the crypto-chip, which attaches itself to the main micro processor and is able to keep the keys away from the connected parts of the device.

Guardtime has invented something called keyless signature infrastructure where they use a hash of a key. A hash is the workhorse of cryptography. You can think of a hash as breaking a plate. It is easy to do in one direction, but it would be hard to put that plate back together to the point where I didn't notice it was broken. They are able to use these tools to authenticate in a much simpler way.

Le sénateur Eggleton : Est-ce cela la cybersécurité?

M. Bauerle : Oui.

Le sénateur Eggleton : C'est donc une solution plus efficace pour se protéger d'une cyberattaque?

M. Bauerle : C'est cet argument voulant qu'il s'agisse d'une loi de la nature. Il y a parfois intérêt à privilégier les choses les plus simples. Dans ce cas, la simplicité de la technologie du bitcoin, et je réalise fort bien qu'elle a l'air compliquée... Si vous l'examinez d'une altitude de 35 000 pieds et la comparez à l'architecture cryptographique traditionnelle, vous avez l'impression qu'il s'agit de quelque chose de confus, d'énorme, qui part dans toutes les directions, et que les clés vont partout, comme lorsque vous voulez acheter quelque chose sur Internet. Si c'est quelque chose que vous pouvez acheter d'un seul clic, et que vous faites marche arrière pour voir ce qui se passe derrière l'écran, tout vous paraît bien emmêlé et confus.

Le sénateur Eggleton : Mais cela ne constitue-t-il pas également une vulnérabilité?

M. Bauerle : C'est certainement le cas. Le fonctionnement des bitcoins finit par ressembler beaucoup à celui d'un distributeur automatique. Vous envoyez tout simplement l'argent. C'est pourquoi les bitcoins sont si importants pour les transactions avec des cartes en plastique, en faisant par exemple la comparaison entre l'argent liquide et les cartes en plastique. Dans ce type de transaction, l'argent est « tiré » d'un compte à un autre. Dans les grandes lignes, vous autorisez une banque à accéder à votre portefeuille, à en retirer de l'argent, à ouvrir le portefeuille de quelqu'un d'autre et à y mettre l'argent. Dans le cas des bitcoins, on procède exactement comme avec de l'argent liquide. Voici l'argent. La transaction est terminée. C'est tout.

Le sénateur Eggleton : Quelles sont les autres difficultés auxquelles on fait face? Le coût en est-il élevé? Est-il probable que le secteur de l'automobile prenne cette voie?

M. Bauerle : Plusieurs entreprises y travaillent déjà. Il y en a une, du nom de Filament, qui a réalisé dès ses débuts dans le domaine de l'Internet des objets qu'il n'existait pas d'équipements pour procéder à des transactions avec des clés. Elle a alors mis au point une pièce d'équipement qu'on peut appeler une cryptopuce qui se fixe sur le processeur principal d'un micro-ordinateur et qui est conçue pour isoler les clés des éléments connectés de l'appareil.

Une autre, Guardtime, a inventé ce qu'on pourrait appeler une infrastructure de signature sans clé dans laquelle elle utilise un fragment d'une clé qui a été « hachée ». La hachure est le cheval de trait de la cryptographie. Pour la visualiser, on peut prendre l'exemple d'une assiette qu'il est facile de casser en plusieurs morceaux, mais dont il est difficile de remettre ensuite les morceaux en place sans pouvoir déceler d'aucune façon les marques de brisure. Ils ont réussi à mettre au point des outils qui parviennent à procéder à l'authentification d'une façon beaucoup plus simple.

Senator Eggleton: So it protects personal information better in terms of access to it. It protects you from cyberattack, by and large. Is it still in an early evolutionary stage?

Mr. Bauerle: Very early stages.

Senator Eggleton: How about the issue of privacy? Will it benefit or will it be a problem? We're concerned about all the data that is being collected in these systems now.

Mr. Bauerle: I included a few of the relevant privacy laws, particularly the EU general regulation on privacy, which is about to take effect in 2018. PIPEDA is in harmony with this law. That law suggests that almost any information that can be tied back to an individual is counted as personal information and therefore subject to the penalties of this new EU regulation.

But there are two other super important parts of this regulation. They talk about security by design. This one is the super wide scope slide I sent you guys. The second one is something called privacy by design and by default, and I'll read you what the law says: "Encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if privacy is to be achieved."

This is followed by the general directives under which the privacy law was written, and that says, "If the personal data is pseudonymised with adequate internal policies and measures by the data controller, then it is considered to be effectively anonymised, and not subject to the controls and penalties" of this new regulation.

So it's my belief that because bitcoin is anonymous, pseudonymous — and other cryptocurrencies are anonymous — but the architecture can be used in such a way that we can anonymize users, machines in particular, and that authentication comes with their use of keys that they are able to automatically comply with privacy law, which is a tremendous advantage, and that's something that I'm here to defend and suggest never changes.

Senator Eggleton: That's good. Let me ask you about one more aspect of this. Is there any impact on publicly-paid-for infrastructure? We're talking about connecting vehicles. We're talking about possibly connecting into street signs, traffic lights or whatever else, as part of the general infrastructure provided

Le sénateur Eggleton : C'est donc une technologie qui permet de protéger les renseignements personnels en bloquant l'accès à ceux-ci. Elle vous protège tout simplement des cyberattaques. Cette technologie en est-elle encore à ses balbutiements?

M. Bauerle : Ils n'en sont qu'au tout début.

Le sénateur Eggleton : Qu'en est-il de la question de la protection des renseignements personnels? Va-t-elle profiter de cette technologie où celle-ci va-t-elle lui poser un problème? Nous sommes préoccupés en voyant la quantité de données que tous ces systèmes recueillent actuellement.

M. Bauerle : Vous trouverez dans mes diapositives des commentaires sur les législations pertinentes en matière de protection des renseignements personnels, et en particulier sur le Règlement général sur la protection des données, le RGPD, de l'Union européenne qui doit entrer en vigueur en 2018. Les dispositions de la LPRPDE sont tout à fait compatibles avec celles de ce règlement. Le texte européen considère en effet que pratiquement tous les renseignements qui peuvent être reliés à une personne sont considérés comme des renseignements personnels et que leur utilisation non autorisée peut faire l'objet de pénalités.

Ce texte comporte également deux autres séries de dispositions de la plus haute importance. Il traite en effet de la « sécurité dès la conception ». C'est ce dont il est question à la diapositive ayant pour sous-titre « Très grande portée » que je vous ai fait parvenir. La seconde série de dispositions peut être coiffée sous le titre « Protection de la vie privée par défaut ou dès la conception ». Voici ce que ce texte en dit : « Il faut effectuer les activités de chiffrement et de déchiffrement localement et non au moyen d'un service à distance, car les clés et les données doivent demeurer sous le contrôle du responsable des données afin qu'on parvienne à assurer quelque protection que ce soit des renseignements. »

Cet énoncé est suivi de directives de nature générale qui ont présidé à la rédaction de la législation sur la protection des renseignements personnels. Elles se lisent comme suit : « Si le contrôleur de données assure le pseudonymat des données personnelles au moyen de politiques et mesures internes appropriées, on estime qu'elles sont rendues adéquatement anonymes et ne sont donc pas sujettes aux contrôles et peines » de ce nouveau règlement.

Le fait que le bitcoin soit anonyme et n'utilise qu'un pseudonyme, alors que les autres cryptomonnaies ne sont qu'anonymes, et que l'architecture du système peut être utilisée de façon à rendre les utilisateurs anonymes, en particulier les machines, et que l'authentification vient de leur utilisation des clés, m'amène à estimer que cette technologie se conforme automatiquement à la législation sur la protection des renseignements personnels. C'est là un avantage énorme et c'est la raison pour laquelle je viens plaider devant vous de ne jamais modifier cette caractéristique.

Le sénateur Eggleton : C'est très bien. Permettez-moi de vous interroger encore sur un autre aspect de toute cette question. Y a-t-il des répercussions sur les infrastructures financées à même les fonds publics? Nous parlons ici de connecter des véhicules entre eux. Nous parlons de la possibilité de leur permettre de lire la

in municipalities. How does this impact on that? Is this all self-contained, or does it require that kind of an investment in infrastructure by public sources?

Mr. Bauerle: I don't think so. I think what might end up working is that the manner in which the technology behaves can be dictated by executive power and legislative power and regulatory power from an executive ministerial level or from a governmental level, but the deployment of this technology can be a commercial opportunity, for example.

Mr. Patterson: Regardless of the foundational cryptography, whether it's classical PKI, bitcoin, anything like that, the cost for adding it to the infrastructure will be approximately the same.

The exact adoption, which systems would, for instance, use bitcoin, and looking at it from a cryptography point of view, I could see having a great deal of applicability for vehicle-to-vehicle communication. You may want to take a look at using more classical authentication models for things like the digital signature of software and the recognition of whether or not this particular software should be trusted to be loaded on this vehicle; or whether or not this particular signal originating from an authoritative source, i.e., a police vehicle, a piece of traffic infrastructure, some other source that is beaming something to that autonomous car. It may end up looking like a mix of the two. So bitcoin for vehicle to vehicle, or to put it more succinctly, blockchain for vehicle to vehicle, and for vehicle to something other than a vehicle, you're looking at using more classical authentication methods.

Mr. Bauerle: Even to illustrate that point for the vehicle-to-vehicle point, there's someone in the bitcoin industry working on this for autonomous vehicles where the vehicle will pay the cars in front of it in the lanes to get out so it can go. This is being developed today. There is no need for the machine to appeal to a third party, which will then negotiate with this other car so that they will beat it. They are just going to pay the guy in front of them, get out of my way, and then pay the next guy to get out of my way, and this is being developed right now.

The Chair: Well, that opens up a whole new bunch of issues.

Senator Galvez: Thank you very much for this very interesting presentation. In the last sessions here, I have been changing my opinion about cars. I have started seeing them more as computers. The more you talk, the more you talk, the more I feel like we will be driving computers.

signalisation routière, les feux de circulation ou quoi que ce soit d'autre qui fait partie des grandes infrastructures mises en place dans les municipalités. Quelles seront les répercussions sur celles-ci? L'ensemble de ce système sera-t-il indépendant ou nécessitera-t-il des investissements en infrastructures dans les services publics?

M. Bauerle : Je ne le crois pas. Je crois que, au bout du compte, les modalités de fonctionnement de cette technologie pourront être dictées par les pouvoirs exécutifs, législatifs et de réglementation, par exemple au niveau ministériel ou au niveau gouvernemental, mais le déploiement de cette technologie pourrait aussi être vu, par exemple, comme une occasion commerciale.

M. Patterson : Indépendamment du type de cryptographie utilisée à la base, qu'il s'agisse d'une infrastructure à clés publiques classique, de celle des bitcoins ou de quoi que ce soit de comparable, le coût de son ajout aux infrastructures sera sensiblement le même.

Si nous en venons maintenant aux modalités précises d'adoption, quels sont, par exemple, les systèmes qui utiliseront la technologie des bitcoins et, du point de vue de la cryptographie, j'imagine très volontiers qu'on trouvera quantité de possibilités d'application aux communications de véhicule à véhicule. Vous voudrez peut-être examiner des modèles plus classiques d'authentification pour des choses comme la signature numérique de logiciels et pour déterminer si un logiciel précis doit ou non être considéré comme fiable pour être téléchargé à bord de ce véhicule, ou pour déterminer si un signal donné provient ou non d'une source faisant foi comme, par exemple, un véhicule de police, un élément d'infrastructure du contrôle de la circulation, ou d'autres sources diverses qui envoient des données vers cette voiture autonome. Au bout du compte, vous aurez peut-être un mélange des deux, la technologie des bitcoins étant utilisée pour les communications de véhicule à véhicule ou, formulée de façon succincte, des chaînes de blocs pour les transmissions de véhicule à véhicule, et pour les communications d'un véhicule à un autre type d'équipement, vous pourrez envisager d'utiliser des méthodes d'authentification plus classiques.

M. Bauerle : Pour illustrer ce point des communications de véhicule à véhicule, je peux même vous dire que quelqu'un dans le secteur des bitcoins travaille à l'application de cette problématique aux véhicules autonomes afin qu'un véhicule qui se trouve dans une voie de circulation paye les voitures qui sont devant lui dans cette voie pour en sortir et poursuivre sa route. C'est un module que quelqu'un est en train de mettre au point. La machine n'a pas besoin de faire appel à une tierce partie, qui négociera alors avec l'autre véhicule pour prendre sa place. Ils vont juste avoir à payer la personne devant eux, pour qu'elle s'écarte de leur chemin, et payer ensuite la suivante pour qu'elle fasse aussi de même. C'est effectivement là un module en cours de développement.

Le président : Eh bien, cela soulève toute une nouvelle série de questions.

La sénatrice Galvez : Je vous remercie de cet exposé fort intéressant. La vision que j'ai des voitures a été modifiée au cours de nos dernières séances. Je commence à les percevoir davantage comme des ordinateurs. Plus vous nous en parlez et plus j'ai le sentiment que nous allons conduire des ordinateurs.

If I go in that direction, I can bring all my worries from the software to this situation, and I will add to my colleague Senator Eggleton saying that we as a government worry about safety, security, privacy, but also consumer protection. Consumer protection is worrying me a lot because there is a lot of planning obsolescence in the industry of software. There is planned obsolescence. It's there, so the consumer has to keep buying and buying and buying, and you just said the guy is there, push him out.

We know that every system can be hacked at a point. We have been blind. It's just a matter of time. We have viruses. We have all kinds of things going into our machines.

You were mentioning that I will have my car, and Tesla is saying it's beaming the data and the software is there and we have to worry about the authentication, who am I, and am I downloading what I want to download? Are you suggesting that, at a point, if I'm not downloading or I'm not authenticating the right things, I will need somebody to come and help me out? My colleague the other day said what happens with the Canadian Tire and the mechanics that come? Who will help me out? Will it be a telephone and down beam me and I'm blocked for some time? Can you please tell me, reassure me?

Mr. Patterson: The way I would look at it is this moving them to being more autonomous platforms is actually good for the consumers, and the reason being is we can look at the Tesla model again. You can upgrade; they are sending upgrades to your car. If you bought a model 90D a few years ago, it didn't have autopilot. Now it does, so you're getting a free feature. Since it's now software, this isn't something where we need to go and add a module to the car or anything like that. In a certain way, it's adding to the life of the vehicle. You can also get a performance upgrade. You just simply pay them their extra \$2,000 and all of a sudden your car will accelerate from 0 to 60 in four seconds instead of nine seconds. We'll argue whether that's a safe thing or not, but some people like it.

With regard to the fact that they are now computers, yes, they are, and we're not going to get away from that. That's how we're getting to the point of having efficient vehicles. We can't build mechanical systems that get the fuel efficiencies and emissions controls that we have. That has to be governed by a computer on

Si je poursuis dans cette direction, je peux appliquer tout ce qui m'inquiète dans le domaine des logiciels à cette situation, et j'ajouterai même à ce que mon collègue le sénateur Eggleton a déjà dit, soit qu'à titre de gouvernement nous devons nous préoccuper de la sécurité, de la protection des renseignements personnels, mais également de la protection des consommateurs. Ce dernier point me préoccupe beaucoup parce qu'on planifie l'obsolescence à grande échelle dans le secteur des logiciels. On y observe vraiment une obsolescence planifiée. Ces logiciels sont construits de telle façon que le consommateur n'a d'autre choix que de continuer à les acheter, et, comme vous venez de le dire, si quelqu'un se trouve devant vous, poussez-le hors de votre chemin.

Nous savons tous fort bien que n'importe quel système peut être piraté à un moment donné. Nous avons été aveugles par le passé, mais ce n'est qu'une question de temps avant que cela se produise. Nous avons des virus et il survient quantité d'autres choses dans nos machines.

Vous nous avez dit que cela concernera un jour ou l'autre ma voiture. On dit que Tesla télécharge déjà des données et des logiciels et cela nous oblige à nous préoccuper des questions d'identification, soit de savoir qui je suis, et si je télécharge bien ce que je veux télécharger. Êtes-vous en train de me dire que, à un moment donné, si je ne télécharge pas le bon élément ou si je ne m'authentifie pas correctement, il faudra que je fasse appel à quelqu'un pour m'aider. Mon collègue nous a raconté l'autre jour ce qui va se passer chez Canadian Tire avec les mécaniciens. Qui va pouvoir m'aider? Faudra-t-il téléphoner à quelqu'un qui va ensuite télécharger l'élément manquant ou suis-je paralysé pendant un certain temps? Pouvez-vous, s'il vous plaît, me rassurer?

M. Patterson : Voici la façon dont j'envisage l'avenir : le fait de les déplacer sur des plateformes plus autonomes est en vérité une bonne chose pour les clients, il suffit pour s'en convaincre de regarder encore une fois comment les choses se passent pour le modèle 90D de Tesla. Vous pouvez mettre à niveau le logiciel de ce véhicule. Tesla envoie des mises à jour à votre voiture. Si vous avez acheté ce modèle il y a quelques années, il n'était pas alors équipé d'un autopilote. Il dispose maintenant de cette fonction, ce qui fait que vous obtenez une caractéristique additionnelle gratuite. Comme les fonctions sont dorénavant commandées par un logiciel, vous n'avez plus à vous rendre au garage pour faire ajouter un module à la voiture. D'une certaine façon, cela revient à prolonger la vie du véhicule. Vous pouvez également obtenir une mise à niveau pour améliorer les performances. Il vous suffit alors de payer un montant additionnel de 2 000 \$ et tout d'un coup votre voiture va accélérer de 0 à 60 km/h en quatre secondes au lieu de neuf. On peut se demander si c'est là une chose sécuritaire ou non, mais il y a des gens à qui cela plaît.

Il est vrai que, dorénavant, nos voitures sont bourrées d'ordinateurs et ce n'est pas là une tendance qui va disparaître. C'est grâce à cette technologie que nous allons pouvoir bénéficier de véhicules efficaces. Nous ne parvenons pas à construire des systèmes mécaniques permettant d'obtenir l'efficacité voulue en

a second-by-second and millisecond-by-millisecond basis. It's got to be a computer doing that, but the thing that we have to take a look at is who can service the parts.

Well, if it's a computer, it will be a matter of taking that computer module off the car, as long as the manufacturer allows the diagnostic codes, which I agree need to be available to every single Joe mechanic in this country, and the ability to purchase that particular computer module and make it modular on and off. The aerospace industry already does this. Flying an airplane now is a whole bunch of computers running Windows and Linux, as interesting and scary as that may sound. The mechanics servicing these airplanes go and get a bare unit out of the warehouse when something breaks on the airplane, puts it in, and then somebody in the engineering department says, "Okay, that particular airplane needs to have the following 27 pieces of software installed on it." That's just what happens. The dealers will probably keep track of which software you're entitled to.

Your mechanic that's at Canadian Tire or your corner mechanic won't be able to add pieces of software for you, but there will definitely be a way, since that module will be able to authenticate that this is a Tesla-certified piece of software or a Ford-certified or Toyota-certified piece of software; why not? It's easy. As I said, it will actually prolong the life of the cars because we will be able to get those features.

Apple comes out with a phone every year. I'm sure they would love me to upgrade it. I still have a three-year-old iPhone, but I'm running the all-but-latest version of their operating system, so I benefited from all those extra upgrades. We are seeing the same thing with the autonomous cars, and we are certainly seeing that with airplanes.

The Chair: Colleagues, I want to remind you that we have a second panel.

Senator Mercer: Thank you, gentlemen, for being here.

Mr. Patterson, I want to continue on a couple of things that you just said, that you didn't think that the mechanic at the local Canadian Tire would be able to fix the car because he wouldn't have access to the software. This is a huge concern. This is another whole industry that goes on, particularly in rural or small-town Canada. If you live in a big city, you have access to dealers, and traditionally car owners don't go back to the dealer because in their mind, whether it's right or wrong, the price is higher at the dealer than it might be at the mechanic down the road. If the mechanic down the road, whether it be at Canadian Tire or the local garage, doesn't have access to this software, we will create a huge employment problem in that industry, and it's an important industry, particularly in small-town and rural Canada.

ce qui concerne le carburant et les émissions. La consommation de carburant et la production des émissions doivent être régies par un ordinateur à la seconde près et même à la milliseconde. Seul un ordinateur peut faire cela, mais nous allons maintenant nous demander qui peut assurer le service des pièces.

Eh bien, s'il s'agit d'un ordinateur, il suffira de retirer le module concerné de la voiture, pourvu que le fabricant donne accès aux codes de diagnostic qui, j'en conviens, devront pouvoir être consultés par n'importe quel mécanicien dans ce pays. Il sera également nécessaire de pouvoir acheter ce module précis d'ordinateur qui devra fonctionner de façon modulaire. C'est ce que fait déjà l'industrie aérospatiale. Faire voler un avion de nos jours revient à utiliser toute une série d'ordinateurs sous Windows et Linux, aussi intéressant et effrayant que cela puisse paraître. Lorsque quelque chose cesse de fonctionner à bord d'un de ces avions, le mécanicien se rend tout simplement à l'entrepôt pour se procurer une pièce unitaire qu'il va mettre à sa place dans la carlingue. Un employé du service technique décide alors qu'il faut installer 27 logiciels à bord de cet avion. C'est ainsi que les choses se passent. Le concessionnaire va probablement vérifier quels sont les logiciels qui peuvent être installés sur votre avion.

Le mécanicien de Canadian Tire ou le mécanicien de votre quartier ne seront probablement pas en mesure d'ajouter des logiciels à votre place, mais il y aura très certainement une façon de le faire puisque ce module pourra attester qu'il s'agit bien là d'un logiciel certifié par Tesla, ou par Ford ou Toyota dans un avenir proche. C'est facile et cela aura pour effet, comme je l'ai déjà dit, de prolonger la durée de vie des voitures parce que nous aurons accès à ces caractéristiques.

Apple sort un nouveau modèle de téléphone tous les ans. Je suis convaincu qu'ils aimeraient beaucoup que je mette le mien à niveau. Cela fait trois ans que je l'ai, mais j'utilise toujours la dernière version de leur système d'exploitation, ce qui fait que je profite de ces mises à niveau additionnelles. Nous voyons la même chose avec les voitures autonomes, comme nous le voyons bien évidemment avec les avions.

Le président : Chers collègues, je vous rappelle que nous avons un deuxième groupe de témoins.

Le sénateur Mercer : Messieurs, je vous remercie d'être venus.

M. Patterson, j'aimerais revenir sur quelques commentaires que vous venez de faire; vous avez dit que vous ne pensiez pas que le mécanicien du magasin Canadian Tire local pourrait réparer ce genre de véhicule parce qu'il n'aurait pas accès aux logiciels nécessaires. C'est une grave préoccupation. C'est un autre grand secteur d'activités, qui s'exerce principalement dans les régions rurales du Canada ou dans les petites villes. Si vous habitez dans une grande ville, vous avez accès aux concessionnaires, et habituellement, les propriétaires de voiture ne font pas entretenir leurs véhicules par le concessionnaire parce que, dans leur esprit, à tort ou à raison, le concessionnaire pratique des prix supérieurs à ceux du mécanicien d'à côté. Si le mécanicien d'à côté, que ce soit un mécanicien de Canadian Tire ou d'un garage local, n'a pas accès

Mr. Patterson: I would say, realistically, the only time the software would need to be reloaded is if the central computer module or one of those computer modules is replaced. Certainly, the committee needs to ensure that the rules are in place to allow the free and fair access to those computer modules by any qualified mechanic and that the manufacturers of those cars don't require a visit to the dealership in order to reload the software. After all, why would you? You're getting the software updates over the air. Theoretically, it should be a matter of taking the old computer module that's faulty — and remember it's only that module. The rest of the parts should just work.

Senator Mercer: You just said the magic words, “free access.” That sounds very good as we're sitting around this table having this discussion, but the people sitting around the table at the boardroom of the company that's producing the software are saying, “Why are we giving away our software free? Why aren't we making Joe mechanic out in rural Canada pay a fee to access that software? He needs it, we've got it, so why not make a dollar as it's going by?” I see a very big risk for the support of rural Canadians and small-town Canadians because of the lack of access. You'll have to help me with that.

You also spoke earlier in your presentation with respect to broad directives, and it sounded good. You talked about broad directives, and we need more specific applications. The directions need to be more specific instead of broad statements. You gave us a broad statement in explaining that to us, so I want you to be a little more specific. Give us an example of something that has happened because of those broad applications instead of specific direction.

Mr. Patterson: All right. So one of the applicabilities was in the transmittal of software to the aircraft. Transport Canada and the FAA have a regulation that simply says if you are transmitting the software over a non-governmental network, you have to take appropriate security controls to ensure the integrity and authenticity of that software. That's the rule. It says nothing. They could have said, “Use the methods in ARINC, which is one of the aerospace standards bodies, ARINC standard 827 and standard 835 and the identity management guidance in ATA spec 42 in order to provide that level of security.”

Senator Mercer: One of my concerns in this whole process is that Canadians are excited — and some are nervous — about the future of autonomous vehicles, et cetera, but I don't know that they have factored in what they sacrifice in the process, namely,

à ces logiciels, cela va créer beaucoup de chômage dans cette industrie, et c'est une industrie importante, en particulier dans les petites villes et dans les régions rurales du Canada.

M. Patterson : Je dirais qu'en pratique, le seul cas où il faudrait peut-être recharger le logiciel serait celui où il faudrait remplacer le module informatique central ou un de ces modules informatiques. Il faudrait bien sûr que le comité veille à ce qu'il y ait des règles qui permettent un accès libre et équitable à ces modules informatiques pour les mécaniciens qualifiés et pour que les fabricants de ces véhicules n'obligent pas leurs propriétaires à se rendre chez leur concessionnaire pour recharger le logiciel. En fin de compte pourquoi cela serait-il nécessaire? Il est aujourd'hui possible de mettre à jour les logiciels par Internet. En théorie, il s'agirait simplement de démonter le module informatique défectueux — et n'oubliez pas que ce n'est qu'un module. Toutes les autres pièces devraient fonctionner.

Le sénateur Mercer : Vous avez prononcé les mots magiques « libre accès ». C'est très facile à dire pour nous qui avons cette discussion en ce moment, mais les gens qui assistent à une réunion du conseil d'administration de la société qui produit les logiciels se disent : « Pourquoi allons-nous donner gratuitement nos logiciels? Pourquoi ne pas demander au mécanicien, Marcel, qui vit dans une région rurale du Canada, de payer quelque chose pour avoir accès à ce logiciel? Il en a besoin, nous l'avons, alors pourquoi ne pas essayer de gagner un peu d'argent de cette façon? » Je crois que le manque d'accès représente un danger très grave pour les petites villes canadiennes et les régions rurales. Vous allez devoir m'aider sur cette question.

Vous avez également parlé plus tôt dans votre exposé de l'adoption de directives générales et cela m'a plu. Vous avez parlé de directives générales, mais vous avez dit que nous avons besoin d'applications plus précises. Il faudrait que les directives soient précises et ne pas se contenter de directives générales. Vous avez exposé les grandes lignes de cette question, mais j'aimerais que vous soyez un peu plus précis. Donnez-nous un exemple de quelque chose qui s'est produit, parce que nous avons des directives générales et non des directives précises.

M. Patterson : Très bien. Une des applications possibles était la transmission d'un logiciel vers un aéronef. Transports Canada et la FAA ont adopté un règlement qui énonce simplement que la transmission d'un logiciel sur un réseau non gouvernemental doit faire l'objet de contrôles de sécurité appropriés pour veiller à préserver l'intégrité et l'authenticité de ce logiciel. C'est le règlement. Il ne dit rien d'autre. On aurait pu dire : « Utiliser les méthodes de l'ARINC, un des organismes qui établit des normes dans le domaine de l'aérospatiale, la norme ARINC 827 et la norme 835 et la directive ATA 42 en matière de gestion des données d'identité pour fournir ce niveau de sécurité ».

Le sénateur Mercer : Ce qui m'inquiète dans tout cela, c'est que les Canadiens sont très intéressés — et certains sont un peu nerveux — par l'avenir des véhicules automatisés, mais je ne sais pas s'ils ont pris en considération le fait qu'ils allaient devoir

information that will be going from the vehicle back to the car manufacturer or the software manufacturer. Somebody will know what's going on.

One of you mentioned speed earlier. If you are someone who is consistently 10 kilometres over the speed limit, that information goes back. Your insurance company says, "Hey, we don't want to insure somebody." Insurance companies are bad enough to deal with. Nobody wants to deal with them. I have a phrase for it. I call it "legalized extortion." You can't do things without insurance, so you have to buy it. You have no choice. You try to shop around, but because they know you have no choice, it's not that competitive a market. Why would I want to give information from my vehicle that would affect my insurance rate, if, for example, I were to be a speeder?

Mr. Patterson: Senator, do you use Google?

Senator Mercer: Rarely.

Mr. Patterson: I saw an article today that says apparently Google's AI algorithms are now able to predict with about 90 per cent accuracy when somebody is going to commit suicide. Google essentially knows every single thing about you. That's their entire business model. Facebook is exactly the same thing.

When we're looking at the privacy rules, we are already giving up, through the use of our phones — for instance, how many here have android phones? You are already giving Google exactly the same telemetry information as your car would. Keep that in mind before we try to say the car can't emit anything that is identifying.

Senator Mercer: All that being said, Mr. Patterson, Canadians don't know that. It's happening, but they don't know it, and they also don't know what the consequences are. I think that's one of my concerns, and this is the Transport and Communications Committee, and on the communication and transportation industries' issues, I think we have a duty to report that if you're going down this road, you are giving up all of this privacy. You are giving up all of this information. You are giving information to people who may turn around and use this against you. For example, in renewing your insurance, they can say, "Well, since you are a constant speeder, we're going to increase your premiums, even though you haven't had an accident in 10 or 15 years, but because you're always 10 kilometres over the speed limit, we're going to increase your premiums," and, of course, they will have the data to back that up.

Mr. Bauerle: Senator Mercer, when it was just discussed that Google's entire business model is aggregating and collecting this information, the business model of many bitcoin and blockchain

sacrifier certaines choses pour obtenir ce service, à savoir l'information qui va aller du véhicule au fabricant ou à celui du logiciel. Il y a quelqu'un qui saura ce qui se passe.

Il y a un d'entre vous qui a parlé de vitesse. Si vous circulez régulièrement à une vitesse supérieure de 10 kilomètres à la vitesse permise, cette information est transmise. Votre compagnie d'assurance va dire : « Hé, nous ne voulons pas assurer ce gars. » Les relations avec les compagnies d'assurance sont déjà très difficiles. Personne ne veut avoir affaire à ces compagnies. J'ai trouvé une expression pour définir ce qu'elles font. J'appelle ça de l'« extorsion légalisée ». On ne peut rien faire sans assurance, de sorte que nous sommes obligés d'en acheter une. Nous n'avons pas le choix. On compare les prix, mais ces compagnies savent fort bien que nous n'avons pas le choix et ce marché n'est donc pas concurrentiel. Pourquoi fournir des renseignements au sujet de mon véhicule, si cela risque de modifier mes primes d'assurance, si, par exemple, je roule trop vite?

M. Patterson : Sénateur, est-ce que vous utilisez Google?

Le sénateur Mercer : Rarement.

M. Patterson : J'ai lu aujourd'hui un article qui semble dire qu'avec ces algorithmes AI, Google est en mesure de prévoir avec une exactitude à près de 90 p. 100 si quelqu'un va se suicider. En fait, Google sait tout sur vous. C'est son modèle commercial. Facebook fait exactement la même chose.

Nous avons déjà renoncé aux règles qui protègent la vie privée lorsque nous utilisons nos téléphones — par exemple, combien d'entre vous possèdent un téléphone avec Android? Vous donnez déjà à Google les mêmes renseignements télémétriques que votre véhicule transmettrait. Pensez à tout cela avant de dire qu'un véhicule ne peut transmettre aucun renseignement touchant l'identité.

Le sénateur Mercer : Monsieur Patterson, c'est que les Canadiens ne le savent pas. Cela se fait, mais ils ne le savent pas, et ils ne savent pas non plus quelles sont les conséquences. C'est une de mes craintes; nous sommes le Comité des transports et des communications, nous parlons des questions qui concernent les industries des transports et des communications et j'estime que nous avons le devoir de faire savoir à la population que nous allons renoncer à protéger la vie privée, si nous nous engageons dans cette voie. Nous fournirons tous ces renseignements. Vous fournissez des renseignements à des gens qui risquent de les utiliser contre vous. Par exemple, si vous renouvelez votre assurance, la compagnie pourrait vous dire : « Eh bien, étant donné que vous conduisez trop vite, nous allons augmenter vos primes, même si vous n'avez pas eu d'accident depuis 10 ou 15 ans, parce que vous dépassez toujours de 10 kilomètres la limite de vitesse; nous allons donc augmenter vos cotisations. » Et bien entendu, ces compagnies auront les données qui justifient leur décision.

M. Bauerle : Sénateur Mercer, nous venons de dire que le modèle commercial de Google consiste à accumuler et à recueillir des renseignements, mais le modèle économique de nombreuses

companies is the opposite. It's to negotiate this data where privacy is first and that users can control the data themselves.

The announcement that Toyota Research Institute mentioned here about blockchain technology and was announced at our conference in New York three weeks ago was precisely that. They are using a start-up called BigchainDB, which is able to coordinate this information to use to help set standards, pass standards, but it also blinds it. It also ensures that you're not sharing unnecessary information, that you're not doing exactly what you're worried about — sharing too much.

So it coordinates the relevant information for those who need it and is able to actually tear away parts of the transaction and blind the rest and leave the person who needs to know the very limited amount of information that's required to get that, but everything else becomes hidden. One of the main purposes of a lot of these companies is to address exactly what you are talking about, that you don't have to give away your entire life just to speed up a little on the highway.

Senator Mercer: However, Mr. Bauerle, what puzzles me about bitcoin is that the attractiveness is the security, but the public concern should be the security. If there's wealth moving around in the world and nobody's monitoring this, and wealth is moving from a legitimate operation to an illegitimate operation to a criminal operation, or what have you, somebody needs to know about it. And by having this privacy, you can't do it.

Mr. Bauerle: The on- and off-ramps are pretty well regulated around the world. From cash into crypto, there's a lot of KYC and all traditional business methods that go on. The senator mentioned before that every system is hackable, and you just mentioned no one is watching bitcoin. Bitcoin is secured by half a billion dollars of computers competing to earn bitcoin by adding security to the network. The computers themselves that make up the bitcoin network are doing the work of the security. Bitcoin has never been hacked, and they are spending zero dollars on security, not a penny, because that is the business model. Computers are sitting there staring at a public ledger, which did something different. It created digital property. It made something digital scarce, limited. Before that, things that were digital could be copied and pasted. It was very easy. Ask the music industry or the movie industry. Digital meant ephemeral, unlimited. It was an oxymoron to call something limited and digital, but all these computers that are attached to the network — I've even forgotten the metric. Bitcoin has been around for seven years and has attracted more computing power than the 10,000 largest banks in the world combined, seven or eight times more than Google itself, and it's very new. These computers, their entire purpose, their entire reason for being is the security of the network. That's the point of these computers coming. They are sitting staring at this information,

sociétés de bitcoin et de chaîne de blocs est tout à fait à l'opposé. Il s'agit de négocier ces données en donnant la priorité à la vie privée et en fournissant aux utilisateurs la possibilité de contrôler eux-mêmes les données.

L'annonce que vient de faire le Toyota Research Institute au sujet de la technologie des chaînes de blocs et qui a été mentionnée au cours de notre conférence tenue à New York, il y a trois semaines, portait précisément sur cet aspect. Il s'agit d'une start-up appelée BigchainDB, qui est capable de coordonner ces renseignements pour établir et faire adopter des normes, mais aussi pour anonymiser ces données. Cela permet de ne pas transmettre les renseignements qui ne sont pas nécessaires, et d'éviter de faire exactement ce que vous craignez — communiquer trop d'information.

Ce processus permet de coordonner les renseignements pertinents destinés à ceux qui en ont besoin et est en fait capable d'anonymiser certaines parties de l'opération, tout en laissant la personne qui a besoin de renseignements, un accès à une quantité très limitée d'information, mais tout le reste est occulté. Un des grands objectifs d'un bon nombre de ces sociétés consiste à répondre directement à votre préoccupation, à savoir que vous ne voulez pas que soient diffusés tous les renseignements vous concernant pour simplement accélérer un peu les choses sur les routes.

Le sénateur Mercer : M. Bauerle, ce que je ne comprends pas très bien au sujet du bitcoin est que cette monnaie est intéressante à cause de la sécurité, mais le public devrait se préoccuper de la sécurité. S'il y a une monnaie qui circule dans le monde et que personne ne la surveille, si cette monnaie passe d'une opération légitime ou à une opération illégitime, et ensuite, à une opération criminelle, ou autre, il faudrait que quelqu'un le sache. Mais en assurant le respect de la vie privée, vous ne pouvez pas le faire.

M. Bauerle : Les accès et les sorties sont assez bien réglementés dans le monde. Lorsqu'on passe de l'argent en espèces à l'argent crypté, on utilise beaucoup le principe KYC, connaître votre client, et toutes les autres méthodes commerciales traditionnelles. Le sénateur a déjà mentionné qu'on pouvait pirater n'importe quel système et vous venez de dire que personne ne surveille le bitcoin. Le bitcoin est surveillé par plus d'un demi-milliard de dollars d'ordinateurs qui se font concurrence pour gagner des bitcoins en renforçant la sécurité du réseau. Ce sont les ordinateurs qui constituent le réseau du bitcoin qui assurent la sécurité. Le bitcoin n'a jamais été piraté et il ne dépense pas un seul centime sur la sécurité, à cause de son modèle commercial. Les ordinateurs sont là en train d'examiner un registre public, qui a fait quelque chose de différent. Il a créé des biens numériques. Il a rendu rare et limité un élément numérique. Auparavant, on pouvait toujours copier et reproduire tout ce qui était numérique. Cela était très facile. Parlez-en à l'industrie de la musique ou à celle du cinéma. Numérique voulait dire éphémère et illimité. C'était un oxymore de dire que quelque chose était limité et numérique, mais tous ces ordinateurs qui sont reliés au réseau — et j'ai même oublié le métrique. Le bitcoin existe depuis sept ans et a attiré une puissance informatique supérieure à celles des 10 000 plus grandes banques prises ensemble, qui représente sept ou huit fois la puissance de

waiting for people to move keys. And if one makes a transaction that is not authorized, the network will find out right away because they are competing to tell — the analogy you can use to understand this —

The Chair: I want to remind you, we have a second panel.

Mr. Bauerle: I'll leave it there and maybe come back to it.

Senator Marwah: This is a question for Mr. Bauerle. I see that CoinDesk specializes in the subject of bitcoin and its underlying technology blockchain. Is the view that for bitcoin to get traction in a material sense, meaning where it becomes part of a global currency, that it needs to be regulated? Is that an oxymoron? How do you regulate something that is built to not be regulated?

Mr. Bauerle: I think it is already regulated by math. The math regulates it.

Senator Marwah: But I'm talking about government, in terms of central banks. I'm talking about that's the regulation. Do you believe there's a role for governments to play there, or is it really a role that's not required?

Mr. Bauerle: In the end, it's just cryptographic keys being passed between people, and I'm not sure how you could regulate that other than saying you can use it for this or that. There's nothing that a government can do that would make a system that is so elegant to begin with better than it already is. There are technical applications, but the idea of regulating — maybe a cash-to-crypto conversion, that's already being regulated. That's being regulated all over the world, but regulating the use of cryptographic keys is impossible. It's a key.

Senator Marwah: How about regulating in the sense of being part of national currency? We have a Canadian dollar.

Mr. Bauerle: That would be fine.

Senator Marwah: How do you regulate something like bitcoin in a country like Canada? It's impossible. I would like to hear your thoughts on how you bring it into a national exchange services.

Mr. Bauerle: Bitcoin was three technologies. It was the cryptographic keys, the network and the program that runs the actual authorization of transactions. These three technologies coordinate. They are orchestrated in a particular way.

Think of a bicycle for a second. When the first bicycle was invented, none of the parts were new. It was the orchestration that was magic, the idea that this thing on two wheels could have momentum and go forward. That can be regulated all people

Google et c'est tout nouveau. Ces ordinateurs n'ont qu'un seul objectif, assurer la sécurité du réseau. C'est la raison pour laquelle il y a tous ces ordinateurs. Ils surveillent constamment ces renseignements, attendent que des gens appuient sur les clés. Si quelqu'un fait une opération qui n'est pas autorisée, le réseau le découvre immédiatement parce qu'ils se font tous concurrence — la comparaison que je peux faire pour expliquer cela est...

Le président : Je tiens à vous rappeler que nous avons un deuxième groupe de témoins.

M. Bauerle : Je vais en rester là quitte à y revenir plus tard.

Le sénateur Marwah : Ma question s'adresse à M. Bauerle. Je vois que CoinDesk se spécialise dans le bitcoin et la technologie qui en est à la base, la chaîne de blocs. Peut-on affirmer que, si l'on veut que le bitcoin démarre vraiment, qu'il fasse partie d'une monnaie mondiale, il faut le réglementer? Est-ce un oxymore? Comment réglementer quelque chose qui a été conçu pour ne pas être réglementé?

M. Bauerle : Je pense que le bitcoin est déjà réglementé par les mathématiques. Ce sont les mathématiques qui le réglementent.

Le sénateur Marwah : Mais je parle des gouvernements, des banques centrales. Je parle de réglementation. Pensez-vous que les gouvernements devraient jouer un rôle dans ce domaine ou que cela n'est pas nécessaire?

M. Bauerle : En fin de compte, ce sont simplement des clés cryptographiques qui passent d'une personne à l'autre, et je ne vois pas très bien comment cela pourrait être réglementé, à moins tout simplement de dire que l'on peut l'utiliser pour une certaine chose et pas pour une autre. Le gouvernement est absolument incapable d'améliorer un système aussi élégant. Il y a des applications techniques, mais l'idée de réglementer — peut-être la conversion d'espèces en monnaie cryptée, mais cela est déjà réglementé. Cela est réglementé partout, mais il est impossible de réglementer l'utilisation des clés cryptographiques. C'est une clé.

Le sénateur Marwah : Et si on réglementait cela en l'intégrant à notre monnaie nationale? Nous avons le dollar canadien.

M. Bauerle : Ce serait très bien.

Le sénateur Marwah : Comment réglementer quelque chose comme le bitcoin dans un pays comme le Canada. C'est impossible. J'aimerais savoir si vous avez des idées sur la façon de l'intégrer à nos services d'échange nationaux.

M. Bauerle : Le bitcoin est associé à trois technologies. Il y a les clés cryptographiques, le réseau et le programme qui s'occupe d'autoriser les transactions. Ces trois technologies sont coordonnées. Elles sont orchestrées d'une certaine façon.

Pensez un instant à la bicyclette. Lorsque la première bicyclette a été inventée, aucune des pièces n'était nouvelle. C'est leur regroupement qui était magique, l'idée que cette chose qui reposait sur deux roues pouvait prendre de l'élan et avancer. On peut bien

want. They can add these technologies in this same combination, in this same orchestration, the same way bitcoin did, because no one owns the idea of a bicycle; it's just out there.

The genius of bitcoin was the orchestration and arrangement of these technologies. That was the, "Aha, if you do it that way, it works." So central banks are absolutely free to copy this orchestration to their heart's desire, and they can do all kinds of wonderful things, and they are doing all kinds of wonderful things. The Bank of Canada is heavily involved testing this stuff. They have tried to put part of the Canadian dollar in its native digital form so that there would be part of the money supply that does not have a paper equivalent and that is digital to its core. This can be used for settlement and all kinds of things. The largest banks in the world have all created their own network together called the distributed ledger, which is basically the same arrangement as bitcoin but without the coin being minted.

This can be deployed, used and copied to any government's heart's desire. They can continue to do this for years to come, and they will. That's effectively what people in my industry believe, that this orchestration of cryptographic tools will continue for many years and represents a true revolution in the way we deploy cryptography.

Senator Mercer: I want to come back to the issue of the security of bitcoin and people, and I don't mean individual citizens but police forces and bank regulators understanding where this wealth is being moved. We're not talking about simple information; millions or billions of dollars can be moved via bitcoins, and without proper regulations or supervision. It could be moved into or out of drug cartels. It could be moved into criminal organizations or terrorism organizations. This is the concern that people have when the movement of large volumes of wealth is not regulated. That's why we have central banks. That's why we have regulations, to protect the common good. The common good is to protect us all, so I need you to explain to me why bitcoin should be excluded from the protection.

Mr. Bauerle: We have banks all around the world that are doing nothing but. Take Canada with FINTRAC provisions. They have to report every transaction above \$10,000. They can't trace one single prosecution from all of this reporting that banks and co-ops and all these small outfits are doing. They are just reporting into this big void, and all this is going on every single day.

Police have to do their jobs. They have to catch money launderers and criminals, but we have a public health epidemic on our hands with private data, and it will get worse. If we rig connected cars the same way we have organized our online banking, we're in big trouble. It's not going to work. We're going

essayer de réglementer une telle chose, mais on ne peut utiliser ces technologies de la même façon, avec le même agencement, tout comme l'a fait le bitcoin, parce que personne n'est propriétaire de l'idée de la bicyclette; cette idée existe tout simplement.

Le bitcoin est génial parce qu'il réussit à harmoniser et à agencer le fonctionnement de ces technologies. Il y a eu ceci : « Eh bien, en le faisant de cette façon, cela fonctionne. » Les banques centrales ont donc toute latitude de copier cette structure, et de faire toutes sortes de choses merveilleuses et elles font déjà toutes sortes de choses merveilleuses. La Banque du Canada est en train de faire de nombreuses études sur cette question. Elle a essayé de donner à une partie de la masse monétaire une forme numérique pour l'intégrer à cette masse, mais sans support papier; un élément entièrement numérique. Cela peut servir pour les compensations et ce genre de choses. Les principales banques ont créé leur propre réseau qu'elles appellent le registre distribué, qui est pour l'essentiel identique à celui du bitcoin, mais sans qu'il y ait production de bitcoin.

Ce système peut être déployé, utilisé et copié par tous les gouvernements. Ils peuvent continuer à le faire à l'avenir et le feront. C'est ce que croient les représentants de mon industrie, à savoir que cette harmonisation des outils d'encryptement va continuer longtemps et représentera une véritable révolution dans la façon dont nous utilisons la cryptographie.

Le sénateur Mercer : J'aimerais revenir sur la question de la sécurité du bitcoin et des gens, et je ne parle pas des citoyens, mais des services de police et des autorités de réglementation des banques qui veulent savoir où aboutit cette richesse. Il ne s'agit pas ici de simple information; il est possible de transférer des millions ou des milliards de dollars en bitcoins, et ce, sans aucune surveillance ou véritable réglementation. Ces sommes pourraient être versées à des cartels de la drogue ou versées par eux. Elles pourraient être transférées à des organismes criminels ou terroristes. Les gens s'inquiètent que l'on déplace de grandes quantités de richesse sans que cela soit réglementé. C'est la raison pour laquelle nous avons des banques centrales. C'est la raison pour laquelle nous avons des règlements, pour protéger le bien commun. Le bien commun consiste à nous protéger tous, c'est pourquoi je voudrais que vous m'expliquiez pourquoi il faudrait soustraire le bitcoin à cette protection.

M. Bauerle : À l'heure actuelle, il y a, dans le monde entier, des banques qui ne font que ça. Prenez le Canada et les dispositions du CANAFE. Les banques doivent déclarer toutes les opérations supérieures à 10 000 \$. Toutes les déclarations qu'effectuent ces banques, les coopératives et tous ces petits établissements n'ont jamais débouché sur une seule poursuite. Ces opérations sont déclarées et disparaissent dans un grand vide, et c'est ce qui se passe tous les jours.

La police doit faire son travail. Elle doit appréhender les criminels et ceux qui font du blanchiment d'argent, mais nous sommes aux prises à l'heure actuelle avec une épidémie publique reliée aux données privées, et la situation ne pourra que s'aggraver. Si nous relient nos véhicules connectés comme nous l'avons fait

to expose ourselves even more. It's one thing to have a couple hundred bucks stolen from your credit card; it's another thing entirely to have your car out of control on the highway.

Sure, financial regulation is really important and there are tools that will not go away. Investigators and police will all be there, and that doesn't need to go anywhere. But arranging the security of this just so someone can call the cops when they know something's wrong is not as good as baking the security into the technology itself. It certainly does allow a vehicle for some of this stuff that you talked about, but more importantly, it protects our privacy.

So you have to weigh the two, and it is a one or the other in some cases. Not in every case. There are many different examples, but if you introduce a third party just to make sure this reporting goes on, you might be leading the whole system down a path where it can be corrupted very easily. You end up increasing the surface area of attack, which is extremely dangerous.

The Chair: And a final statement, Mr. Patterson?

Mr. Patterson: I would say that regardless of what the cryptographic underlying underpinnings are, whether that is blockchain or PKI, regardless, the piece that needs to really be elucidated by Transport Canada and regulated for this is cars should be first and foremost trusted computing environments. If this software did not come from someone, it should not be executable, which means even if somebody finds a vulnerability and manages to load a piece of software onto your radio or into your car's navigation system, if that piece of software wasn't signed by the automotive manufacturer or one of his designated authorized software producers, it should not be executable. That is a fundamental security practice that needs to be applied to autonomous vehicles, the same way as we do for aircraft and the same way we are beginning to do for trains. We need to segregate the networks and make sure we have a trusted computing environment.

[Translation]

The Chair: I would like to thank Mr. Patterson and Mr. Bauerle for being with us today.

[English]

We are continuing our study on connected and automated vehicles. I am pleased to introduce our next witness, from Ford Canada, Mr. Blake Smith, Director for Sustainability, Environment and Safety Engineering.

[Translation]

Thank you for being here. We are ready to hear your opening remarks.

pour les opérations bancaires en ligne, nous allons avoir de graves problèmes. Cela ne fonctionnera pas. Nous allons être de plus en plus vulnérables. Se faire voler quelques centaines de dollars à cause de sa carte de crédit est une chose, mais perdre complètement le contrôle de sa voiture sur la route est une chose tout à fait différente.

Bien sûr, la réglementation financière est très importante et il y a des outils qui seront toujours là. Les enquêteurs et les policiers seront toujours là, mais il n'est pas nécessaire d'aller plus loin. Assurer la sécurité d'un tel système en donnant à chacun la possibilité d'appeler les policiers en cas de problème n'est pas la même chose que d'intégrer la sécurité dans la technologie. C'est un moyen que l'on peut utiliser pour certaines des choses dont vous avez parlé, mais surtout, cela protège notre vie privée.

Il faut donc concilier les deux et dans certains cas, il faut même choisir entre les deux. Pas toujours. Il y a beaucoup de situations différentes, mais si vous introduisez un tiers pour être sûr que les déclarations sont faites, cela risque d'amener le système à suivre une voie où il sera très facile de le corrompre. En fin de compte, cela augmente les risques d'attaque, ce qui est extrêmement dangereux.

Le président : Une dernière déclaration, monsieur Patterson?

M. Patterson : Je dirais que, quelles que soient les techniques cryptographiques de base utilisées, qu'il s'agisse de chaînes de blocs ou de PKI, l'aspect que Transports Canada doit examiner et réglementer c'est la sécurité des environnements informatiques de ces véhicules. Si la source d'un logiciel est inconnue, il ne devrait pas pouvoir être exécuté, ce qui veut dire que, même si quelqu'un trouve une vulnérabilité et réussit à charger un logiciel dans votre radio ou dans le système de navigation de votre véhicule, si ce logiciel n'a pas été signé par le fabricant du véhicule ou par l'un des producteurs de logiciel autorisés et désignés, il ne devrait pas pouvoir être exécuté. C'est une technique de sécurité fondamentale qu'il faut appliquer aux véhicules automatisés, tout comme nous le faisons pour les aéronefs et comme nous commençons à le faire pour les trains. Il faut séparer les réseaux et faire en sorte que notre environnement informatique soit sécurisé.

[Français]

Le président : J'aimerais remercier M. Patterson et M. Bauerle de leur présence parmi nous aujourd'hui.

[Traduction]

Nous poursuivons notre étude sur les véhicules branchés et automatisés. J'ai le plaisir de présenter notre prochain témoin, Blake Smith, directeur en chef, Durabilité, environnement et ingénierie de la sécurité, Ford du Canada limitée.

[Français]

Merci d'être avec nous. Nous sommes prêts à entendre votre présentation.

[English]

Blake Smith, Director, Sustainability, Environment and Safety Engineering, Ford Motor Company of Canada, Limited: I'd like to preface my remarks with a couple of overview comments. From a Ford perspective, when we talk about connected and automated vehicles, it's really about making things better for our customers and, ultimately, making a better world. It is in that context that I am making my comments. If it doesn't do that, it shouldn't be done.

Good morning, and thank you, honourable senators. More than 100 years ago, Ford was founded with a clear vision, and that was really around making people's lives better by making transportation accessible to everyone, democratizing transportation.

The innovations at Ford have helped to make car ownership a reality for millions, advanced human progress, enabled people to become more connected with each other and to find greater opportunities to live, work and play where they want, make personal choices. It was a revolution in connecting average people, the likes of which we haven't seen again until recently.

In Canada, Ford has been part of the fabric since 1904. In addition to our current \$700 million investment in our manufacturing facilities, we recently announced a \$500 million research and development investment. Approximately 300 software and hardware engineers have been added to our mobility team in Ottawa, Waterloo and Oakville. Our mobility team is the development group looking at new ways for people to move. That's the connection. These folks are part of the connected and automated vehicle space.

At Ford, our approach to automated driving is to pursue both a bottom-up approach, where we focus on adding features that provide drivers with increasing levels of automation — think about adaptive cruise control, automated emergency braking, those sorts of features that are add-ons to existing vehicles that we are familiar with — and the top-down approach, where we focus on a high level of autonomy and where the vehicle does the driving for the driver or for the person that is in control of the vehicle.

For most people, autonomous vehicles are a new idea. Trust is really important. Ford has spent the past century earning that trust. We know how to make safe, quality vehicles at high volumes, to meet varying needs of people around the world.

We have an extensive design, development and verification process to ensure the high quality and performance of all of our products. These include analyzing the intended function, identifying user experiences and performing robustness and durability testing, including modelling, track and real-world driving.

[Traduction]

Blake Smith, directeur, Durabilité, environnement et ingénierie de la sécurité, Ford du Canada limitée : J'aimerais préfacier mes remarques par quelques commentaires généraux. Du point de vue de Ford, les véhicules branchés et automatisés doivent nous permettre d'améliorer les choses pour nos clients et, en fin de compte, améliorer la situation générale. C'est dans ce contexte que je présente mes commentaires. Si ce n'est pas là l'effet de ces recherches, alors elles ne méritent pas d'être faites.

Bonjour et merci aux honorables sénateurs. Il y a plus d'un siècle, Ford a été fondé dans un but très clair; il s'agissait d'améliorer la vie des gens en offrant un moyen de transport accessible à tous et en démocratisant le transport.

Les innovations qui ont été faites par Ford ont permis à des millions de personnes de se procurer un véhicule, elles ont fait progresser l'humanité, elles ont permis aux gens d'être mieux reliés aux autres, d'avoir davantage de possibilités pour vivre, travailler et jouer où ils le souhaitent, et de faire des choix personnels. Cela a révolutionné la façon de relier les citoyens ordinaires entre eux, et ce n'est que tout récemment que nous avons constaté une évolution semblable.

Au Canada, Ford fait partie de la fibre de ce pays depuis 1904. En plus d'un investissement actuel de 700 millions de dollars dans nos établissements industriels, nous avons récemment annoncé un investissement de 500 millions de dollars pour la recherche et le développement. Nous avons ajouté près de 300 spécialistes en logiciels et matériel à notre équipe de mobilité à Ottawa, Waterloo et Oakville. Notre équipe de mobilité est un groupe qui explore d'autres façons de transporter les gens. C'est le lien. Ces gens font partie du monde des véhicules branchés et automatisés.

Chez Ford, l'approche à la conduite automatisée est une approche ascendante, grâce à laquelle nous ajoutons des mécanismes qui automatisent de plus en plus la conduite — pensez au régulateur de vitesse adapté, aux freins d'urgence automatiques, ce sont là des dispositifs qui s'ajoutent aux véhicules que nous connaissons bien — et une approche descendante qui est axée sur l'acquisition d'une grande autonomie pour que le véhicule conduise le conducteur ou la personne qui contrôle le véhicule.

Pour la plupart des gens, les véhicules automatisés sont une idée nouvelle. La confiance est un aspect extrêmement important. Cela fait un siècle que Ford cherche à gagner la confiance des gens. Nous savons comment construire en grand nombre des véhicules sûrs et de qualité, de façon à répondre à tous les besoins de la population mondiale.

Nous utilisons des processus de vérification, de développement et de conception complexes pour que tous nos produits soient de grande qualité et performants. Cela veut dire analyser la fonction souhaitée, identifier l'expérience de l'utilisateur et effectuer des tests de durabilité et de robustesse, notamment en utilisant des modèles ainsi que la conduite sur circuit et sur route.

Autonomous vehicles will be held to the same high prove-out standard. They do, of course, have some unique attributes that will require some additional considerations. As such, we believe that self-certification, which is the methodology used in North America, is the best path forward as we continue to work with regulators on these types of vehicles.

Public trust can also be earned by establishing pilots with specific geofenced areas or mapped areas where the vehicles are confined. This will provide much needed interaction with the public to influence the perception about self-driving vehicles. In the U.S., our team has been partnered with a variety of cities to implement new mobility services, including fully autonomous vehicles. I am optimistic that this will extend to Canada in the future.

We are also actively engaged with the U.S. National Highway Traffic Safety Administration, NHTSA for short, and other stakeholders to provide data and policy considerations that may help to inform their views on autonomous vehicles. We support NHTSA's federal automated vehicle policies and appreciate Transport Canada's continued collaboration with NHTSA as policy is further developed.

Ford looks forward to continued work with the Canadian government on developing a national framework and policies to enable deployment of transportation as a service, using the SAE Level 4 vehicles without driver controls. The U.S. and Canada have a shared driving environment, so it just makes sense to have aligned approaches. This is really an extension of the way we have operated for a very long time.

Ford will look very different in the next 5 to 10 years if it meets its intent to put autonomous vehicles on the road by 2021. According to recent remarks by Bill Ford, "We should be less capital intensive, less cyclical, much closer to the customer, and help cities sort out their issues. We will be making vehicles. It is something we do and we do well. . . But how they behave, how they interact and who is in them may all be different."

This is a transformational moment in the industry, perhaps the most transformational moment of the past century, and we look forward to being part of it.

Senator Mercer: Thank you very much, Mr. Smith, for being here; we appreciate your time.

Les véhicules autonomes devront respecter les normes habituelles, qui sont éprouvées et très exigeantes. Ils possèdent bien sûr des caractéristiques uniques qui appellent d'autres considérations. Dans ce domaine, nous pensons que l'autocertification, qui est la méthode utilisée en Amérique du Nord, est la meilleure solution et nous continuons à travailler avec les autorités de réglementation sur ces types de véhicules.

Nous pourrions également gagner la confiance de la population en lançant des projets pilotes dans des secteurs délimités sur le plan géographique ou cartographique à l'intérieur desquels les véhicules devront demeurer. Nous apprendrons ainsi, ce qui est très utile, comment réagissent les gens de façon à influencer leur perception des véhicules autonomes. Aux États-Unis, notre équipe a établi des partenariats avec un certain nombre de villes pour mettre en œuvre de nouveaux services de mobilité, y compris les véhicules entièrement automatisés. Je suis convaincu que ces services seront offerts au Canada à l'avenir.

Nous travaillons également étroitement avec la U.S. National Highway Traffic Safety Administration, NHTSA pour faire plus court, et d'autres parties prenantes pour leur présenter notre point de vue sur les politiques et les données afin d'alimenter leur point de vue sur les véhicules autonomes. Nous appuyons les politiques fédérales de la NHTSA en matière de véhicules automatisés et nous sommes heureux de constater que Transports Canada continue à collaborer avec la NHTSA dans le domaine de l'élaboration de ces politiques.

Ford est heureux de continuer à travailler avec le gouvernement canadien à l'élaboration de politiques et d'un cadre national qui permettent le déploiement du transport à titre de service, en utilisant des véhicules conformes à la norme SAE niveau 4 qui ne contiennent pas de mécanismes de contrôle pour le conducteur. Les États-Unis et le Canada ont le même environnement routier et il est donc logique que leurs approches soient harmonisées. Ce n'est en fait que le prolongement de la façon dont nous fonctionnons depuis très longtemps.

Ford aura beaucoup changé d'ici 5 à 10 ans, s'il réussit à mettre sur la route des véhicules autonomes en 2021. D'après des commentaires récents prononcés par Bill Ford : « Notre société ne devrait pas s'appuyer autant sur l'investissement, elle doit être moins cyclique, plus proche du consommateur et elle devrait aider les villes à régler leurs problèmes. Nous fabriquons des véhicules. C'est ce que nous faisons et nous le faisons bien... Mais la façon dont ces véhicules se comporteront et interagiront, et qui se trouvera à l'intérieur de ces véhicules sera peut-être très différente. »

Notre industrie se trouve à un moment charnière, c'est peut-être le moment le plus important de ces 100 dernières années et nous sommes heureux de le vivre.

Le sénateur Mercer : Monsieur Smith, je vous remercie d'être venu; nous l'apprécions.

You mentioned earlier in your presentation about the verification process and how important it was. Can you give us a little more detail about the verification process that Ford is looking at and how that will work from the point of view of the company?

Mr. Smith: Perhaps you could help me a little bit. I guess I can do it from a couple of angles. I can talk about how we layer security; I can talk about privacy. When it comes to the automated vehicle space —

Senator Mercer: The answer to the question is all of those.

Mr. Smith: Okay. First and foremost, we believe that data belongs to the person in control of the vehicle. We also believe in an approach that treats different kinds of data differently. For example, today, the systems for the so-called OBD port on a vehicle, for its emission control setup and so on, is a port that vendors can plug into and service the vehicle. Obviously, that level of security is not adequate for some other system. The approach is unique to the system. These are layered systems.

Our security control approach is what you call defence in depth layered technique. You isolate systems, and you have them layered. Then, if any system is violated, for whatever reason, it sets off some form of signal. I didn't want to answer specifically, of course, because our product development process is proprietary. That is a place we can't go too far on, but I did want to give you a sense of how we try to deal with that.

On different kinds of data, I think there will be different values for different purposes. Obviously, people's truly personal information they should have control of. I will use how my cellphone connects to my vehicle today. I make a choice about whether I connect, whether I let my contacts load into my vehicle. That's a choice. I choose to put mine in because then I can do what I do while I drive. It is the same with text. Once I have done that, though, and I turn my vehicle in, I have to have the presence of mind to delete it. Otherwise, it could be exposed. The individual has a role to play as does the company.

Over-the-air updates involves a choice, again. The system will identify that an update is available. You can choose to subscribe for the update or you can choose to wait and make a choice on an individual basis. That's the sort of approach. Leave the decision with the data owner.

There is public good, however, in some forms of data. If it's properly handled or anonymized, for example, in the current world, that data could be used to smooth traffic, for example. If vehicles are connected, over a period of time the system can learn to operate more efficiently. There is a public good. Part of

Vous avez parlé plus tôt dans votre exposé de votre processus de vérification et de son importance. Pouvez-vous nous en dire davantage au sujet du processus de vérification que Ford est en train d'étudier et de la façon dont il fonctionne du point de vue de votre société?

M. Smith : Vous pourriez peut-être m'aider un peu. Je peux répondre à cette question de divers angles. Je peux vous parler des niveaux de sécurité; je peux vous parler de la protection de la vie privée. Pour ce qui est du monde des véhicules automatisés...

Le sénateur Mercer : La réponse à ma question devrait englober tous ces aspects.

M. Smith : Très bien. Premièrement et principalement, nous pensons que les données appartiennent à la personne qui contrôle le véhicule. Nous pensons également qu'il faut traiter différemment les données qui sont différentes. Par exemple, aujourd'hui, les systèmes associés au port OBD du véhicule, pour le réglage du contrôle des émissions notamment, sont un port dans lequel les vendeurs peuvent se brancher et entretenir le véhicule. Bien évidemment, ce niveau de sécurité n'est pas suffisant pour d'autres systèmes. Chaque approche est particulière à chaque système. Ce sont des systèmes stratifiés.

Notre approche au contrôle de la sécurité est ce que nous appelons une défense axée sur une technique stratifiée. On isole les systèmes et on les stratifie. De sorte que, s'il est porté atteinte à un système, quelle que soit la raison, cela déclenche un signal. Je ne souhaite pas vous donner trop de détail bien sûr parce que notre processus d'élaboration de nos produits est exclusif. C'est un domaine dans lequel je ne peux pas vous en dire trop, mais je voulais vous donner une idée de la façon dont nous abordons cette question.

Pour ce qui est des différents types de données, je dirais que nous leur appliquerons différentes valeurs pour différentes fins. Bien évidemment, c'est l'individu qui doit avoir le contrôle des renseignements qui sont véritablement personnels. Je décide de la façon dont mon téléphone cellulaire est relié à mon véhicule aujourd'hui. Je fais le choix de me relier, et de charger ma liste de contacts dans le véhicule. C'est un choix. Je choisis de le faire parce que cela me permet ensuite de continuer à faire ce que je fais lorsque je conduis. C'est la même chose avec les messages. Lorsque j'ai terminé et que je rends mon véhicule, je dois avoir la présence d'esprit de supprimer ces données. Elles risqueraient autrement d'être piratées. L'individu a un rôle à jouer, tout comme la société.

Les mises à jour en direct se font, elles aussi, à la suite d'un choix. Le système signale qu'il existe une mise à jour. Vous pouvez choisir d'accepter la mise à jour ou d'attendre et de faire ce choix plus tard. C'est le genre d'approche que nous adoptons. Il faut laisser cette décision au propriétaire des données.

Il y a malgré tout certaines formes de données qui sont reliées au bien public. Si elles sont bien traitées ou anonymisées, par exemple, il y a actuellement des données que l'on pourrait utiliser pour faciliter la circulation, notamment. Lorsque les véhicules sont connectés, le système peut apprendre, avec le temps, à les exploiter

the discourse of public policy has to be how do we do that in a manner that protects the individual's privacy so that an individual's location or speed or whatever isn't identified but it's part of a data set that can be used to communicate back to vehicles that are automated and make traffic smooth, flow more evenly, avoid an accident, et cetera.

Senator Mercer: My final question, Mr. Smith, is one that we have asked a number of people because this committee has dealt in the past with the licensing and issuing of spectrum by the government. Are you convinced that Ford's efforts in this industry will not be hindered by the lack of spectrum availability to allow you to communicate with vehicles?

Mr. Smith: My understanding is that ISED has moved to protect the frequency or is in the process of moving to clear the frequency that would be used for vehicle-to-vehicle communication in North America. I think Canada is going in the right direction. We continue to discuss that with them, obviously. If vehicle-to-vehicle communication becomes a regulation in Canada, that will obviously be very important.

Senator Mercer: But is there enough spectrum available to allow that communication to happen?

Mr. Smith: It's a specific frequency, and that frequency is protected.

Senator Mercer: We now have 50 per cent of the vehicles on the road that have this capability, and everyone wants to communicate with everyone. That is system overload. In particular, if there needs to be communication because of weather, accidents or something, that could put a strain on the system. I assume that in your research there is a stress management process when there is stress on the system?

Mr. Smith: First, vehicle-to-vehicle communication is one very specific corner of the connected vehicle space. Vehicles will be connected with the outside world in several different ways in all likelihood. My vehicle today is connected through its cellphone interface. Presumably there will be more than one connection in the future.

Senator Griffin: One thing I was pleased to see in your presentation was that you could help cities sort out their issues. I used to be a municipal councillor, so I am interested in how you see that happening.

Mr. Smith: As we move to a more shared economy and mobility as a service and a shared transportation model, if congestion is to be lessened, there needs to be fewer vehicles. That is something as a company we are willing to acknowledge and state is important in the long haul.

de façon plus efficace. Cela est pour le bien de la population. La discussion au sujet de ces orientations doit porter sur la façon dont nous obtenons ces résultats en protégeant la vie privée de l'individu et éviter que la vitesse, l'emplacement ou une autre caractéristique de l'individu soient divulgués, mais il faudrait que cela fasse partie d'un ensemble de données qui puisse être utilisé pour communiquer avec les véhicules automatisés, faciliter la circulation, la rendre plus fluide, éviter les accidents, par exemple.

Le sénateur Mercer : Monsieur Smith, ma dernière question est celle que nous avons posée à un certain nombre de témoins parce que le comité s'est déjà occupé de la question des permis associés aux bandes de fréquences et à leur attribution par le gouvernement. Êtes-vous certain que les efforts que déploie Ford dans ce domaine ne vont pas être gênés par l'absence de fréquences disponibles dont vous auriez besoin pour communiquer avec les véhicules?

M. Smith : Je crois savoir que l'ISDE a pris des mesures pour protéger certaines fréquences ou est en train de libérer les fréquences susceptibles d'être utilisées pour les communications entre véhicules en Amérique du Nord. Je pense que le Canada va dans la bonne direction. Nous continuons à en parler avec le ministère, bien évidemment. Si la communication entre les véhicules est réglementée au Canada, cela deviendra bien évidemment très important.

Le sénateur Mercer : Mais y a-t-il suffisamment de fréquences pour que cette communication soit possible?

M. Smith : C'est une fréquence spécifique et c'est cette fréquence qui est protégée.

Le sénateur Mercer : À l'heure actuelle, la moitié des véhicules en circulation peuvent utiliser cette technique et tout le monde veut communiquer avec tout le monde. Le système est surchargé. En particulier, s'il fallait communiquer à cause des conditions climatiques, des accidents ou d'autres choses, cela pourrait surcharger le système. Je tiens pour acquis que votre recherche porte également sur les processus de gestion du stress lorsque le système subit un stress.

M. Smith : Premièrement, la communication entre les véhicules est un aspect très particulier du monde des véhicules connectés. Les véhicules seront connectés au monde extérieur de différentes façons, c'est ce qui est probable. Aujourd'hui, mon véhicule est connecté au moyen de mon téléphone cellulaire. On peut penser qu'à l'avenir, il n'y aura pas qu'un seul genre de connexion.

Le sénateur Griffin : Il y a un aspect de votre exposé qui m'a fait plaisir; c'était le fait que vous êtes en mesure d'aider les villes à régler leurs problèmes. J'ai été conseiller municipal et j'aimerais savoir comment vous pensez que cela pourrait se faire.

M. Smith : Nous nous dirigeons vers une économie où le partage prend de l'importance et nous adoptons un modèle de partage du transport; si nous voulons réduire les encombrements, il faudra qu'il y ait moins de véhicules sur la route. C'est une réalité que notre société est bien sûr prête à reconnaître et elle estime que c'est un aspect important à long terme.

Automated vehicles have the potential to be supportive of multimodal public transportation. We own a service called Chariot that is based in San Francisco which is a van sharing type arrangement that can support public transportation where it is absent. It is connected with train services like the GO Train or Via. As different types of transportation move forward, the ideal would be for those systems to be able to communicate with each other. There is no point in the Chariot service showing up 10 minutes early or 10 minutes late. Those systems are able to communicate with each other. There is an efficiency opportunity.

Senator Griffin: As part of the process for this planning, I'm assuming that you have done consultation with municipalities and with provinces possibly, too?

Mr. Smith: It's early days. The discourse is a little further along in the U.S. than it is in Canada, so we have an opportunity. We are talking to some provinces and some municipalities about what the future might look like. Each of them is going to have to make their decisions about how they want to participate.

Senator Griffin: Yes. That is very important for their planning.

What do you see as the continuing role of the after market? That is, the Canadian Tires of the world and the local service station, especially in rural areas?

Mr. Smith: I have listened to some of the testimony. Folks tend to refer to these rolling computers. Fair enough, but they still have wheels, tires, brakes and steering systems — those are all mechanical systems. Yes, the electrification and the computing power of vehicles continues to go up, but they are still mechanical systems that will require service. What has happened with service generally over time as vehicles have gotten more robust is they require service less frequently. There are fewer and fewer conventional service technicians and more and more higher level technicians that are capable of dealing with the most advanced systems. Tires last longer; exhaust systems last longer — everything last longer. As the quality of vehicles in terms of durability has improved, the need for service has gone down.

[Translation]

Senator Saint-Germain: It is very interesting to hear you talk about the durability and longevity of your cars in the new context. This leads me to wonder about the nature of the warranties you will offer to consumers, and therefore to the buyers of your self-driving vehicles. How will the warranties you provide change? For instance, will the warranty be longer for the computer parts, since the durability and longevity will be longer? Will there be a warranty on the security of the system? By that, I mean the ability to maintain the confidentiality of

Les véhicules automatisés peuvent compléter le transport public multimodal. Nous sommes propriétaires d'un service appelé Chariot, qui est en place à San Francisco; c'est une entente de partage de fourgonnettes qui peut remplacer le transport public lorsqu'il n'y en a pas. Ce service est relié au service ferroviaire comme le GO Train ou VIA. Ces différents types de transport vont continuer à évoluer et il serait souhaitable que ces différents systèmes soient capables de communiquer entre eux. Il ne sert à rien que le véhicule du service Chariot arrive 10 minutes trop tôt ou 10 minutes trop tard. Ces systèmes peuvent communiquer entre eux. Cela donne la possibilité d'en renforcer l'efficacité.

Le sénateur Griffin : Dans le cadre de cette planification, je tiens pour acquis que vous avez consulté les municipalités et même les provinces?

M. Smith : Nous en sommes encore au tout début. La discussion a progressé davantage aux États-Unis qu'au Canada et nous avons donc là des possibilités. Nous avons parlé à quelques provinces et à quelques municipalités de ce que pourrait être l'avenir. Ce sera à tous ces intervenants de décider de la façon dont ils souhaitent participer à ce travail.

Le sénateur Griffin : Oui. C'est très important pour leur planification.

Quel sera, d'après vous, le rôle que continuera de jouer le marché des pièces de rechange? C'est-à-dire les magasins Canadian Tires et les garages locaux, en particulier dans les zones rurales.

M. Smith : J'ai écouté certains témoignages. Les gens font souvent référence à ces ordinateurs sur roulette. C'est vrai, mais il y a encore des roues, des pneus, des freins et des systèmes de direction — qui sont tous des systèmes mécaniques. Il est vrai que l'électrification et la composante informatique des véhicules ne font que se développer, mais il y aura toujours des systèmes mécaniques à entretenir. Graduellement, les véhicules sont devenus plus robustes et ils n'ont pas besoin d'être entretenus aussi souvent. Il y a de moins en moins de mécaniciens conventionnels et de plus en plus de techniciens spécialisés qui sont capables de s'occuper des systèmes les plus perfectionnés. Les pneus durent plus longtemps; les systèmes d'échappement durent plus longtemps — tout dure plus longtemps. La qualité des véhicules s'est améliorée sur le plan de la durabilité, et ce qui a réduit d'autant les besoins d'entretien.

[Français]

La sénatrice Saint-Germain : Il est très intéressant de vous entendre parler de la durabilité et de la longévité de vos automobiles dans le nouveau contexte. Cela m'amène à vous interroger sur la nature des garanties que vous allez offrir aux consommateurs, donc aux acheteurs de vos véhicules autonomes. Qu'est-ce qui va changer dans l'évolution des garanties que vous fournissez? Par exemple, pour la partie ordinateur, la garantie sera-t-elle plus longue, puisque la durabilité et la longévité seront allongées? Y aura-t-il un volet de la garantie sur l'étanchéité des systèmes? J'entends par là la capacité

consumer-entered data. Please tell us about anything else you currently have to consider in developing your warranties to be consistent with the vehicles as they evolve.

[English]

Mr. Smith: The company will have a role in its warranty policy, and I think it's far too soon to predict what that will look like. There is always a role for public policy and the regulator in this space. The basic requirements of the Motor Vehicle Safety Act require us to make sure that vehicles don't have defects or, if they do, they have to be corrected. There are those sorts of obligations, and it is the same on the environmental side. There is an interplay with public policy and the regulator in those spaces.

I assume that as we get more and more learning about technology in the lower levels of automation, when the benefits are clear, the regulator will probably set a minimum standard and make it part of the regulatory landscape. To the extent that any of the systems affect either the safety or environmental elements, those are already in place. As we go forward, I am sure there will be a dialogue about what is essential to be covered and what is less important from a minimum standard of operation.

[Translation]

Senator Saint-Germain: In the interest of both the company and the consumer, you said:

[English]

It is far too soon to think about the guarantees.

[Translation]

Will it be necessary to adapt the warranties that you will give upon the purchase of a car — which today is basically built according to traditional mechanics — to cars that will be like computers on wheels? Have you thought about how you will tailor the warranties you will offer to consumers for these vehicles that will have a much higher price than traditional mechanical cars?

[English]

Mr. Smith: It's not even clear at this point for fully autonomous vehicles what the ownership model is likely to look like. For example, I don't know whether most autonomous vehicles will belong to private individuals or service providers. That is an interesting question. Will they need service? No doubt. How extensive it is, I think, is part of the learning. As vehicles get more electrified and more controlled by electronics, the level of

de conserver la confidentialité des données entrées par le consommateur. Parlez-nous de tout autre élément dont vous devez tenir compte présentement dans l'évolution de vos garanties en conformité avec l'évolution des véhicules.

[Traduction]

M. Smith : La société va jouer un rôle avec sa politique de garantie, mais je crois qu'il est bien trop tôt pour prédire la forme qu'elle pourrait prendre. Les politiques publiques et les autorités de réglementation auront toujours un rôle à jouer dans ce domaine. Les obligations de base de la Loi sur la sécurité automobile nous demandent de faire en sorte que les véhicules n'aient pas de défaut et que, s'ils en ont, ils soient corrigés. Il y a ces sortes d'obligations et il en va de même du côté de l'environnement. Les politiques publiques et les autorités de réglementation interagissent dans ces domaines.

Je pense qu'à mesure que nous améliorons nos connaissances technologiques sur l'automatisation de base, un domaine où les avantages sont évidents, l'autorité de réglementation va certainement établir une norme minimale et l'introduire dans le régime de réglementation. Dans la mesure où ces systèmes touchent les aspects sécurité ou environnement, il y a déjà des règlements. À l'avenir, je suis certain qu'il y aura des discussions au sujet des aspects essentiels à couvrir et des aspects qui sont moins importants pour ce qui est d'une norme minimale de fonctionnement.

[Français]

La sénatrice Saint-Germain : Tant dans l'intérêt de la compagnie que du consommateur, vous avez dit ceci :

[Traduction]

Il me paraît prématuré de penser aux garanties.

[Français]

Deviendra-t-il nécessaire que les garanties que vous donnerez à l'achat d'une automobile — qui, aujourd'hui, est essentiellement construite selon la mécanique traditionnelle — soient adaptées à des voitures qui seront semblables à des ordinateurs sur roues? Avez-vous réfléchi à la façon dont vous adapterez les garanties que vous offrirez aux consommateurs pour ce véhicule qui aura un prix beaucoup plus élevé que les voitures de mécanique traditionnelle?

[Traduction]

M. Smith : Nous ne savons même pas en ce moment quel sera le modèle de propriété des véhicules pleinement automatisés. Par exemple, je ne sais pas si la plupart des véhicules autonomes appartiendront à des particuliers ou à des fournisseurs de service. C'est une question intéressante. Faudra-t-il les entretenir? Certainement. Nous apprendrons à mesure quel sera exactement le genre d'entretien nécessaire. Les véhicules seront de plus en plus

maintenance should go down, not up. They are likely to require some software upgrades from time to time, and the service model for that, at least in my mind, isn't clear yet.

Senator Galvez: Thank you, Mr. Smith, for being here. We understand that car companies will remain the builders of the mechanics of the car. However, there are a lot of software security companies coming forward to ensure communication in the Internet of things. As you said, it is a layered system. There is the inside of the car, then vehicle-to-vehicle, plus vehicle-to-infrastructure and then the vehicle to the satellite for positioning.

I want to get your opinion on this. Having so many players that have the knowledge but not necessarily the control, as they are the developers of this software, there are fractures by which hacking or privacy problems or fraud can be allowed. I want to give you an example.

The gentleman before you said something that was disturbing. He said that you have a car and you can go at this speed, but if you have an update, you can make it faster. If my car had the potential of doing this mechanically by paying for updating the software so I will then be able to go faster, that worries me. It worries me that the mechanics and capacity are enhanced by a software program but that is not told to the customer from the beginning.

I was just thinking about what happened to Volkswagen. They had a problem with their emissions, and this was a software problem. Through the software they could control the emissions reading at various speeds. There was fraud there.

What is Ford thinking about this issue with respect to so many software companies and the layers which are there? If there is a problem, what part of the responsibility will Ford take?

Mr. Smith: First, Ford has the privilege of having been voted one of the most ethical companies in the world eight years in a row. That's something we are quite proud of and we take it very seriously. Having said that, it is incumbent on us as the manufacturer to take responsibility for those sorts of things. In our development protocols, we have ways of doing that. We have also voted with our pocketbook to a certain extent by adding, just as recently as March, 400 engineers from another company, a half-billion-dollar investment. We bought companies that build the LiDAR system. We are insourcing what we view as critical operations. We have long-standing relationships with companies like QNX in Canada that help us with software. It's about making sure that that the business relationship is set up in a manner that deals with those things.

Senator Galvez: Do you see a role for government in ensuring this?

électriques et contrôlés par des composantes électroniques, ce qui devrait dire qu'il y aura moins d'entretien et non davantage. Il faudra probablement mettre à jour les logiciels de temps en temps et le modèle de service qui permettrait de le faire n'est pas encore très clair, du moins dans mon esprit.

La sénatrice Galvez : Monsieur Smith, je vous remercie d'être venu. Nous savons que les sociétés automobiles continueront à construire les aspects mécaniques du véhicule. Il y a toutefois de nombreuses sociétés qui s'occupent de la sécurité des logiciels et qui proposent d'assurer la communication avec l'Internet des objets. Comme vous l'avez dit, c'est un système stratifié. Il y a l'intérieur du véhicule, la communication entre véhicules, la communication entre véhicules et l'infrastructure et ensuite, la communication entre le véhicule et le satellite pour le positionnement.

J'aimerais avoir votre avis sur cette question. Avec autant d'acteurs qui ont accès à ces données sans les contrôler nécessairement, puisque ce sont eux qui ont élaboré le logiciel, il y aura des failles qui se prêteront au piratage, aux atteintes à la vie privée ou à la fraude. Je vais vous donner un exemple.

L'intervenant qui vous a précédé a dit quelque chose qui m'a troublé. Il a dit que vous avez un véhicule qui peut aller à une certaine vitesse, mais qu'avec une mise à jour, il peut aller plus vite. Si mon véhicule avait la possibilité de le faire mécaniquement, mais qu'en achetant une mise à jour du logiciel, il pouvait aller plus vite, cela m'inquiéterait. Cela m'inquiète que les aspects mécaniques et la capacité du véhicule soient améliorés par un logiciel, mais que le client ne soit pas au courant de tout cela au départ.

Je pensais simplement à ce qui est arrivé à Volkswagen. Cette société avait un problème avec ses émissions et c'était un problème de logiciel. Ce logiciel permettait de contrôler la mesure des émissions selon la vitesse. Il y avait de la fraude.

Que pense Ford du fait qu'il y ait autant de sociétés de logiciel et de différentes strates dans ce domaine; s'il y a un problème, quelle sera la responsabilité que Ford sera prête à assumer?

M. Smith : Premièrement, Ford a le privilège d'avoir été reconnue comme une des sociétés les plus éthiques au monde, huit années de suite. C'est quelque chose dont nous sommes très fiers et que nous prenons très au sérieux. Cela dit, il nous incombe en tant que fabricant d'assumer la responsabilité de ce genre de choses. Dans nos protocoles de développement, nous avons différentes façons d'y parvenir. Nous avons également voté avec notre carnet de chèques, dans une certaine mesure, en ajoutant, en mars dernier encore, 400 ingénieurs d'une autre société, ce qui représente un investissement d'un demi-milliard de dollars. Nous avons acheté les sociétés qui ont construit le système LiDAR. Nous faisons à l'interne ce qui nous paraît être les opérations essentielles. Nous avons depuis longtemps des rapports avec des sociétés comme QNX au Canada, qui nous aident pour les logiciels. Il faut faire en sorte que les rapports commerciaux tiennent compte de ces aspects.

La sénatrice Galvez : Pensez-vous que le gouvernement ait un rôle à jouer dans ce domaine?

Mr. Smith: I'm sure you have heard by now, for example, that there are automated vehicle guidelines in the U.S. They have 15 principles, and there is a set of interactions with government before you move into the space. Certainly there is a role for government in ensuring the policy framework for this sort of technology is right. It can't be cookie-cutter; it will have to be situational. It will be data dependent. It will be what the specific data is.

Ideally, we would find a framework that allows innovation in the space to thrive. At the same time, there has to be a public policy framework that establishes boundary conditions and provides the public confidence that they will be safe and secure and their privacy will be protected. The bonus of autonomous technology will be safety and environment.

Senator Eggleton: We have had a lot of discussion about electrification of automobiles through the computer and through the information systems that are being developed. There has also been the reference to propelling the vehicles forward, electrified vehicles or electrical cars as we have known them in the past. Does Ford see all this going hand in hand, moving from fossil fuels over to electrified vehicles as part of this total electrification?

Mr. Smith: There are supporting elements. They are not mutually inclusive, but they can be supporting. Our prototype autonomous vehicles are, in fact, electrified products because they have the kind of battery capacity that's necessary for the sensor technology and so on. So they have a fairly high electric draw at this stage. Our prototypes are hybrids. Ideally, in the short term, we see them as plug-in hybrids, probably. There is some interplay in that sense. Again, because of the power draw of the technology, that will likely change a little bit over time, so they are mutually supportive, I would say.

Senator Eggleton: That's interesting.

Mr. Smith: And to the extent of connectivity, vehicle-to-vehicle communication, can smooth traffic flow, you would make that electrified technology more efficient because it's not accelerating and decelerating all the time. Again, there is some convergence.

The challenge with anything that has a large battery today is still that it is very expensive, and we're probably 10 years or more away from getting to the point where fully electrified vehicles make economic sense. So it's a journey, and we think it's a really important one, like autonomous vehicles, and it's a decision of over what time frame and so on we want to move forward.

Senator Eggleton: Ten years seems amazing. These electrified vehicles have been around for a long time already.

M. Smith : Je suis certain que vous avez appris que, par exemple, il existe aux États-Unis des lignes directrices concernant les véhicules automatisés. Elles comprennent 15 principes et il y a toute une série d'interactions avec le gouvernement avant que les véhicules prennent la route. Il est évident que le gouvernement a un rôle à jouer pour veiller à ce que le cadre réglementaire soit adapté à cette technologie. On ne peut pas tout uniformiser; il faut tenir compte de la situation. Cela dépendra des données. Et cela dépendra des données spécifiques.

Idéalement, nous souhaiterions un cadre qui favorise l'innovation. Parallèlement, il faut qu'il y ait un cadre public qui fixe des limites et garantisse à la population que la sécurité ne sera pas compromise et que leur vie privée sera protégée. La prime qu'apporte la technologie de l'automatisation touchera la sécurité et l'environnement.

Le sénateur Eggleton : Nous avons beaucoup parlé de l'électrification des automobiles au moyen d'un ordinateur et au moyen des systèmes informatiques qui sont en train d'être mis au point. Il a également été mentionné que cela pourrait propulser les véhicules, qu'il s'agisse de véhicules électrifiés ou de véhicules électriques comme nous les connaissions dans le passé. Est-ce que Ford pense que tout cela va ensemble, et nous allons passer des carburants fossiles à des véhicules électriques dans le cadre de cette électrification générale?

M. Smith : Ce sont des éléments qui se complètent. Ils ne sont pas nécessairement reliés entre eux, mais ils peuvent se compléter. Nos prototypes de véhicules autonomes sont en fait des véhicules électriques parce qu'ils possèdent le genre de batteries suffisamment puissantes pour la technologie des senseurs et le reste. Ils consomment donc pas mal d'électricité pour le moment. Nos prototypes sont hybrides. Idéalement, à court terme, nous aimerions que ce soit des hybrides que l'on puisse brancher, probablement. Il y a une certaine interaction dans ce sens. Encore une fois, étant donné l'électricité que consomme cette technologie, ce qui va probablement évoluer avec le temps, ces aspects sont tout à fait complémentaires, d'après moi.

Le sénateur Eggleton : Voilà qui est intéressant.

M. Smith : Le fait que la connectivité, la communication entre véhicules, puisse faciliter la circulation, renforce également l'efficacité de la technologie électrique, parce que les véhicules ont moins besoin d'accélérer et de freiner. Il y a encore ici une certaine convergence.

Le problème que pose la nécessité d'avoir de grosses batteries est qu'elles coûtent encore très cher, et il faudra attendre encore au moins 10 ans avant d'en arriver au point où les véhicules intégralement électriques seront rentables. C'est donc un voyage et nous pensons que c'est un voyage très important, tout comme les véhicules autonomes, et c'est à nous de décider du calendrier que nous devons nous fixer pour l'avenir.

Le sénateur Eggleton : Dix ans, c'est étonnant. Ces véhicules électriques existent déjà depuis longtemps.

Mr. Smith: You may be aware if you're a historian that Henry Ford worked for Edison, and they were studying and developing electric vehicles in the 1800s.

Senator Eggleton: Still trying to master it.

I want to ask you about cybersecurity because a couple of studies have indicated that manufacturers — not necessarily picking you out or Ford — generally don't seem to be quite on top of this. The McKinsey & Company study said that 75 per cent of executives surveyed — this is in the industry or related components of the industry — did not have a countermeasure strategy in place to respond to a cyberattack. And then U.S. Senator Ed Markey, in his study, found only two manufacturers were able to describe any capabilities to diagnose or respond to an attack in real time. What are you doing to overcome what appears to be either an indifference or just a lack of understanding of what to do?

Mr. Smith: I wouldn't call it indifference, and I don't think there's a lack of understanding. I think the landscape is changing very quickly, and we belong to a set of collaborative efforts to improve that space, so that's ongoing and developing quickly. We're actually quite confident that we'll be able to protect the systems.

Senator Eggleton: You said in your opening remarks that you believe self-certification is the best path forward.

Mr. Smith: Right.

Senator Eggleton: In France, they are apparently considering — I guess it's a government issue — a safe AV label. In the United States Senate, they have also suggested a cyberdashboard label. These are government-sponsored labels that are intended to improve public confidence that the systems will work. However, you seem to suggest self-certification is better.

Mr. Smith: Let me describe what self-certification is, to begin with.

In the U.S. and Canada, we have a system of certifying vehicles that's different than the rest of the world. The motor vehicle safety standards in Canada are set up to be protective of the public, and we take the responsibility for saying they comply. And if they don't, there are consequences, both in terms of recall and correction. But in my view, we're held to a higher standard than the so-called type approval where government authorities review the detailed records and decide whether a vehicle is to be certified or not. It's just a different approach, but it puts a very high onus on the manufacturer.

Senator Eggleton: One of these measures coming out is in the United States Senate at the moment, though.

M. Smith : Si vous êtes historien, vous savez peut-être qu'Henry Ford a travaillé pour Edison, et qu'ils étudiaient ensemble la mise au point de véhicules électriques dans les années 1800.

Le sénateur Eggleton : Et nous n'avons toujours pas résolu ce problème.

Je vais vous poser une question au sujet de la cybersécurité, parce qu'il y a des études qui montrent que les fabricants — et il ne s'agit pas particulièrement de vous ou de Ford — ne semblent pas très conscients de cet aspect. Selon l'étude McKinsey & Company, 75 p. 100 des dirigeants interrogés — dans les entreprises de ce secteur ou dans celui des composantes — n'avaient pas adopté de stratégie capable de contrer une cyberattaque. Il y a également l'étude du sénateur américain Ed Markey, qui indique qu'il n'y avait que deux fabricants qui étaient en mesure de diagnostiquer ou de répondre à une attaque en temps réel. Que faites-vous pour lutter contre ce qui semble être soit de l'indifférence, soit simplement de l'incompréhension au sujet des mesures à prendre?

M. Smith : Je ne parlerais pas d'indifférence, et je ne pense pas que ce soit un manque de compréhension. Je crois que la situation évolue très rapidement et que nous participons à un ensemble d'efforts concertés visant à renforcer ce domaine, de sorte que tout se développe très rapidement. En réalité, nous sommes pleinement convaincus que nous serons en mesure de protéger les systèmes.

Le sénateur Eggleton : Vous avez dit dans vos remarques préliminaires que vous pensiez que la meilleure solution était l'autocertification.

M. Smith : Exact.

Le sénateur Eggleton : Je crois que le gouvernement français envisage de créer un label VA sûr. Le Sénat des États-Unis a également proposé un label « cyber tableau de bord ». Ce sont des labels reconnus par les gouvernements qui ont pour but de rassurer la population en indiquant que les systèmes fonctionnent. Vous semblez toutefois affirmer que l'autocertification est préférable.

M. Smith : Permettez-moi de commencer par vous décrire ce qu'est l'autocertification.

Aux États-Unis et au Canada, nous avons un système de certification des véhicules qui est différent de celui adopté par tous les autres pays. Au Canada, les normes de sécurité applicables aux véhicules à moteur ont pour but de protéger le public et ce sont les fabricants qui ont la responsabilité d'affirmer que ces normes sont respectées. Si ce n'est pas le cas, il y a des conséquences, à la fois sur le plan des rappels et sur celui des mesures correctives. Mais à mon avis, nous devons respecter une norme plus élevée que celle que prévoit le système d'approbation dans lequel les autorités gouvernementales examinent des dossiers détaillés et décident s'il est possible ou non de certifier un véhicule. C'est une approche différente, mais qui impose un fardeau très lourd au fabricant.

Le sénateur Eggleton : Une de ces mesures est quand même sur le point d'être prise par le Sénat des États-Unis actuellement.

Mr. Smith: I can't speak to the label, and I'm not sure what value it would provide. However, we have been quite vocal as a company that this has to be a partnership going forward. We view it as the federal government's role to set the framework that we operate in from a product perspective. It's a provincial jurisdiction to set driver requirements and conditions for use, and we would hope that we would get to a provincial model-type system.

Ontario has done some nice work in trying to lay out the conditions for AV-type use, and they have collaborated in that effort along with the state of Michigan quite a bit. It's not a surprise because that's where a lot of the development work is done. The idea of getting through the CCMDA, getting to a model approach and then letting folks adopt it makes a ton of sense to us so that there's continuity.

And then there's a role for municipalities that have to decide how they want their transportation system to work. There are many challenges for municipalities in terms of infrastructure and infrastructure spending, but the most efficient use of their dollar in the long run will be to have these systems be used most efficiently and have them communicate with each other. The dialogue has to be around how does that work best. Simple things. For example, today there's no connection between a GO train and TTC.

Senator Eggleton: True.

Mr. Smith: A bus doesn't communicate with the subway system. These things are all independent. In the long run, that doesn't make any sense. That's where the efficiencies can come and where the technology suite that's coming into this space can apply.

I want to share one other thing where there's an opportunity. We talk about connected vehicles. It tends to get into an urban discussion. It doesn't have to be that way. There are real opportunities. We operate in India and Africa, in places with very remote communities that are difficult to get at. If vehicles can be connected under those conditions, you can ensure that health care is provided for better. If a vehicle can communicate somebody's vitals back to a hospital or a health care facility, there are a lot of opportunities to make life better for people that wouldn't have it otherwise, or for people to get to work that couldn't get to work otherwise. That's the real opportunity here and, of course, in Canada we have lots of these remote places. We tend to think of remote as central Ontario or Nova Scotia or something. Those aren't remote. It's the real remote places where there may be a big opportunity.

Senator Eggleton: Thank you.

Senator Runciman: I have a few brief questions following up on Senator Eggleton and referencing one of our notes about the U.S. government publishing non-binding guidance on cybersecurity

M. Smith : Je ne peux pas parler du label, et je ne sais pas très bien quelle serait son utilité. Notre société a toutefois fait savoir très clairement qu'il faut établir un partenariat dans ce domaine. Nous pensons qu'il appartient au gouvernement fédéral de fixer le cadre dans lequel nous fonctionnons du point de vue des produits. Les conditions applicables aux conducteurs et en matière d'utilisation relèvent des provinces, c'est pourquoi nous espérons que nous pourrions en arriver à un système provincial basé sur un modèle.

L'Ontario a fait du bon travail pour essayer de fixer les conditions pour l'utilisation d'un véhicule de type VA, et cette province a collaboré sur cette question avec l'État du Michigan. Ce n'est pas surprenant parce qu'il se fait beaucoup de développement dans ce domaine. L'idée de passer par la LCCG, d'en arriver à une approche basée sur un modèle et de laisser ensuite les gens l'adopter me paraît une excellente chose parce qu'elle assure une continuité.

Il y a aussi les municipalités qui doivent décider de la façon dont elles veulent voir fonctionner leur système de transport. Elles font face à de nombreux défis pour ce qui est de l'infrastructure et des coûts d'infrastructure, mais à long terme, il sera plus rentable pour elles que ces systèmes soient mieux utilisés et qu'ils communiquent entre eux. La discussion portera sur la question de savoir quelle est la meilleure façon de faire. Des choses simples. Par exemple, à l'heure actuelle, il n'y a pas de connexion entre le train GO et la TTC.

Le sénateur Eggleton : Exact.

M. Smith : Les autobus ne communiquent pas avec le métro. Tous ces systèmes sont indépendants. À long terme, cela n'est pas logique. C'est là que l'on peut gagner en efficacité et où le progrès technologique qui s'annonce dans ce domaine pourra s'appliquer.

J'aimerais mentionner une autre chose si cela est possible. Nous parlons de véhicules connectés. On a tendance à parler principalement des zones urbaines. Ce n'est pas obligatoire. Il existe de grandes possibilités. Nous fonctionnons en Inde et en Afrique, dans des régions où il y a des communautés très isolées auxquelles il est difficile de se rendre. Si nous réussissons à connecter les véhicules dans ces conditions, cela permettra d'améliorer les soins de santé. Si un véhicule peut communiquer les signes vitaux d'une personne à un hôpital ou à un établissement de soins de santé, il sera alors possible d'améliorer la vie des gens qui n'auraient pas accès à ces soins autrement, ou pour que les gens puissent aller travailler alors qu'ils ne pourraient pas le faire autrement. Cela offre de véritables possibilités et bien entendu, au Canada, nous avons beaucoup de régions isolées. Nous avons tendance à penser que les régions isolées se trouvent au centre de l'Ontario ou en Nouvelle-Écosse ou quelque chose du genre. Ce ne sont pas vraiment des régions isolées. Ce sont dans les régions très isolées que cette technologie offre d'excellentes possibilités.

Le sénateur Eggleton : Merci.

Le sénateur Runciman : J'aimerais poser quelques brèves questions dans le prolongement de celles du sénateur Eggleton et en faisant référence à une de nos notes selon laquelle le

best practices for CVs and AVs. As a follow-up to Senator Eggleton's question, what measures has Ford taken to make cybersecurity an organizational priority? Are you aware of what is happening?

Mr. Smith: All I can tell you is we have. As I said earlier, we're members of a number of consortiums to improve and continue to improve our knowledge in that space. We're part of the Auto-ISAC initiative. We belong to the AV consortium. There are a bunch of these sorts of things.

In fairness, this is a journey. Autonomous vehicles are not the conventional privately owned vehicles. They are intended to operate in a geofenced setting, a geomapped kind of confined space and to be for moving people and goods. They are not the classic vehicle the general public would acquire. Part of the reason we announced early our intent to have autonomous vehicles in 2021 is to ensure that we expose the public to them so they have an opportunity to learn. We continue to evolve our best practices, and they operate in a highly controlled setting where if they need to be updated, or if something needs to change, it can happen quickly.

Senator Runciman: I have been a Ford driver for over 20 years, so I'm a big fan of the company and especially respect the fact that a few years ago, when two of the big three went for bailouts, Ford did not. Kudos for that.

I was talking about the issue of public trust, which you mentioned in your submission, and the role of government. We heard from one of the previous witnesses about a minimal role for government, and, in the past, I have referenced this issue of public trust. General Motors, Volkswagen, Hyundai and a number of major manufacturers have kept problems from the public — some of them are now in litigation — that have resulted in deaths. I question this whole issue with respect to public trust. We're only made aware of some of these through whistle-blowers. I have put the question in terms of at least in the initial decade or so of moving in this direction, we should perhaps have a more involved role of government, especially when you look at all these potential security threats involved with automated vehicles as well. I'm just putting to you that this whole public trust issue is, I think, questionable given the actions of some significant manufacturers.

Mr. Smith: From our perspective, we view this space as one where it will have to be a partnership. There is a role for the regulator in the space for sure. That's what the regulator's role is, to ensure public safety.

gouvernement des États-Unis a publié des lignes directrices non obligatoires sur les bonnes pratiques en matière de cybersécurité pour les VC et les VA. À titre de suivi sur la question qu'a posée le sénateur Eggleton, quelles sont les mesures que la société Ford a prises pour faire de la cybersécurité une priorité organisationnelle? Êtes-vous au courant de ce qui se fait?

M. Smith : Je peux tout simplement vous dire que c'est le cas. Comme je vous l'ai déjà dit, nous sommes membres d'un certain nombre de regroupements qui ont pour but d'améliorer et de continuer à améliorer nos connaissances dans ce domaine. Nous participons à l'initiative Auto-ISAC. Nous sommes membres du consortium VA. Il y a toutes sortes de choses de ce genre.

Il faut admettre que c'est un voyage. Les véhicules autonomes sont différents des véhicules conventionnels qui appartiennent à un particulier. Ils sont conçus pour fonctionner dans un environnement délimité, un espace géographique circonscrit et leur but est de transporter les personnes et les marchandises. Ce ne sont pas des véhicules classiques, du genre que la population souhaiterait acheter. Nous avons annoncé très tôt notre intention de lancer les véhicules autonomes en 2021, parce que nous voulions notamment que le public s'habitue à ces véhicules et qu'ils les connaissent mieux. Nous continuons à élaborer de bonnes pratiques et ces véhicules fonctionnent dans un milieu contrôlé dans lequel il est possible d'apporter rapidement des mises à jour ou des changements, en cas de besoin.

Le sénateur Runciman : Cela fait plus de 20 ans que je conduis une Ford, je suis donc un très grand fan de cette société et je respecte en particulier le fait qu'il y a quelques années, deux des trois grands de l'automobile ont demandé à être renfloués alors que Ford ne l'a pas fait. Cela mérite des félicitations.

J'ai parlé de la question de la confiance du public, aspect que vous avez mentionné dans votre mémoire ainsi que du rôle du gouvernement. Nous avons entendu un des témoins précédents parler du fait que le gouvernement devrait jouer un rôle mineur et j'ai déjà abordé la question de la confiance du public. General Motors, Volkswagen, Hyundai et un certain nombre de constructeurs se sont abstenus de signaler certains problèmes au public — problèmes dont certains font l'objet à l'heure actuelle d'un contentieux et qui ont entraîné des victimes. Je me pose beaucoup de questions au sujet de la confiance de la population. Nous n'apprenons ces choses que lorsque des lanceurs d'alerte les signalent. Je pense qu'au moins pendant les premières 10 années de travail dans ce domaine, nous devrions peut-être demander au gouvernement d'intervenir davantage, en particulier, compte tenu de toutes les menaces potentielles que posent pour la sécurité les véhicules automatisés. Je vous mentionne simplement que toute la question de la confiance de la population soulève de graves questions, compte tenu de la façon d'agir de certains constructeurs importants.

M. Smith : De notre point de vue, nous considérons que ce domaine appelle l'établissement d'un partenariat. La réglementation a effectivement un rôle à jouer dans ce domaine. C'est le rôle qui incombe aux autorités de réglementation, à savoir assurer la sécurité du public.

Senator Runciman: Currently, it hasn't been working, obviously, in some instances, with pretty severe results.

Mr. Smith: The systems need to evolve with time, for sure.

I will not comment on other companies' issues for sure, but the way to proceed is to get a good set of oversight parameters in place, and if there are deficiencies in those oversight parameters as technology changes, then obviously it will stress conventional regulators some because technology is moving at a faster pace than they move. It will require some new models. Certainly, though, Mr. Ford in particular has been quite vocal about the need for public policy to develop in a way that allows that trust to develop in the technology.

Senator Runciman: In terms of the long-term viability of the industry in Canada and the serious questions surrounding that, do you have any recommendations you can make in terms of distinguishing that in Canada? It's a very integrated industry, and we know that. But in terms of legislatively or through regulation policy development rather than simply opening the bank vault, what can we recommend to government with respect to ensuring, as best we can, the long-term viability of the industry in Canada?

Mr. Smith: If we're talking about the manufacturing industry, obviously we need a competitive operating environment, and there are some issues in that space at present.

Senator Runciman: And you don't care to get into them today?

Mr. Smith: I'm here to talk about automated vehicles.

Senator Runciman: I would like to hear about that sometime in the future.

Mr. Smith: Sure. There are, obviously, efficiencies in manufacturing when there is an alignment of requirements, and obviously technology is cheaper to the end consumer when there's efficiency. Certainly, I am a long-time advocate of getting the requirements right, but also of internationally, both on a continental basis within North America and on a global basis, moving towards harmonized requirements. Harmonization shouldn't be a dirty word. It's about getting the best requirements and aligning them.

History is the biggest enemy of harmonization, by the way. This is why when we have new spaces, like electrification, fuel cell vehicles, automated vehicles, we're starting from basically ground zero, and then there really is an opportunity to move it on an aligned international basis.

[Translation]

Senator Cormier: Thank you for your presentation. I am interested in the impact of the arrival of self-driving cars on the employment and labour sector. You said, on the one hand, that

Le sénateur Runciman : À l'heure actuelle, il est évident que cela n'a pas toujours bien fonctionné et que cela a entraîné des résultats très graves.

M. Smith : Il faut que les systèmes évoluent, c'est évident.

Je ne vais pas faire de commentaire sur les problèmes qui touchent les autres fabricants, mais la solution me paraît devoir consister à mettre sur pied toute une série de paramètres de surveillance et s'il apparaît des lacunes dans ces paramètres de surveillance en raison de l'évolution de la technologie, alors cela posera des problèmes aux autorités de réglementation conventionnelle, parce que la technologie évolue plus rapidement qu'elles. Il faudra adopter d'autres modèles. Je dirais néanmoins que M. Ford, en particulier, a clairement déclaré à plusieurs reprises qu'il fallait adopter des orientations qui permettront à la population d'avoir confiance dans cette nouvelle technologie.

Le sénateur Runciman : Pour ce qui est de la viabilité à long terme de l'industrie au Canada et des graves questions que cela pose, pouvez-vous faire des recommandations à ce sujet pour le Canada? Cette industrie est fortement intégrée et nous le savons. Mais sur le plan législatif ou sur celui de l'élaboration de règlements par opposition à l'octroi de subventions, que pouvons-nous recommander au gouvernement pour que cette industrie soit viable à long terme au Canada?

M. Smith : Si nous parlons du secteur de la fabrication, il est évident qu'il faut que l'environnement soit concurrentiel, et il se pose certains problèmes dans ce domaine à l'heure actuelle.

Le sénateur Runciman : Et vous ne souhaitez pas les aborder aujourd'hui?

M. Smith : Je suis venu pour parler des véhicules automatisés.

Le sénateur Runciman : J'aimerais en apprendre davantage à un moment donné sur ce sujet.

M. Smith : Bien sûr. On peut, bien évidemment, faire des économies dans le domaine de la fabrication lorsque les conditions sont harmonisées et il est également évident que la technologie coûte moins cher au consommateur final lorsque les opérations sont rentables. Je suis, depuis longtemps, partisan d'adopter des conditions strictes, mais également de préparer l'adoption de conditions harmonisées au palier international, et aussi en Amérique du Nord et à l'échelle mondiale. L'harmonisation ne devrait pas être une insulte. Il s'agit de découvrir quelles sont les meilleures règles à adopter et de les intégrer.

L'histoire est le plus grand ennemi de l'harmonisation, je le dis en passant. C'est pourquoi il y a de nouveaux domaines comme l'électrification, les véhicules alimentés à l'hydrogène, les véhicules automatisés, dans lesquels nous partons pratiquement de zéro, ce qui offre la possibilité réelle d'harmoniser les règles entre tous les pays.

[Français]

Le sénateur Cormier : Merci pour votre présentation. Je m'intéresse à l'impact de l'arrivée des voitures autonomes sur le secteur de l'emploi et de la main-d'œuvre. Vous avez dit, d'une

the cars were going to be more and more durable. You also said that they will need less and less maintenance. So we can imagine that this will have an impact on vehicle manufacturing.

On the one hand, I wonder how your business plan will take these factors into account. What interests me first and foremost is the impact of these changes on the workforce. What do you think the main impacts will be? I am thinking, for instance, of small contractors, small garage owners in the regions. Considering that the cars will be more durable and will need less maintenance, how can the federal government help this industry prepare for this change?

[English]

Mr. Smith: First of all, I guess it would be fair to say that as vehicle technology evolves, it will continue to get more durable and last longer and continue the trend towards fewer people needed in the service industry. That's just a fact. There will be some displacement.

The larger issue may be that as freight in particular becomes more automated, then there may be some displacement of the driver community, and that is a very large source of employment. Some folks will likely be displaced, and so that transition is something that will have to be looked at going forward.

From a business planning perspective, it's too early for me to speak to that in the sense that we're talking about a fully autonomous entry level 4 vehicle in 2021. That's a long way out from a business planning perspective. It will be a vehicle that's used, as I said, in a geofenced environment, so the first vehicle won't likely have a huge volume. It will be more piloting and getting the public to see the technology, start to get comfortable with it, that sort of thing. Impacts are probably further down the road from a business planning perspective, for example, if we looked at our manufacturing footprint.

[Translation]

Senator Cormier: Do you have any ideas about how the federal government could help this sector's workforce anticipate or prepare for this transition and change?

[English]

Mr. Smith: I'm an optimist, so I think that over time, as business models change, employment will shift away from some of those conventional jobs to less conventional jobs. I just don't know what they are yet. I think that's a space that certainly the federal government can watch, and they would no doubt be more knowledgeable than I am about what those options are.

part, que les voitures allaient être de plus en plus durables. Vous avez aussi dit que les besoins d'entretien seraient de moins en moins grands. On imagine donc que cela aura un impact sur la production de véhicules.

D'une part, je me demande comment votre plan d'affaires tiendra compte de ces facteurs. Ce qui m'intéresse avant tout, c'est de savoir quel sera l'impact de ces transformations sur la main-d'œuvre. À votre avis, quels seront les principaux impacts? Je pense, par exemple, aux petits entrepreneurs, aux petits garagistes qui travaillent dans les régions. Considérant que les voitures seront plus durables, qu'elles auront moins besoin d'entretien, comment le gouvernement fédéral peut-il aider ce secteur d'activité à se préparer à cette transformation?

[Traduction]

M. Smith : Premièrement, je crois que l'on peut dire qu'à mesure que la technologie de ces véhicules évoluera, que ces véhicules seront plus robustes et dureront plus longtemps, il y aura besoin de moins d'employés dans le secteur de l'entretien. C'est un fait. Il va y avoir un déplacement des emplois.

La question plus vaste est peut-être qu'étant donné que le transport de marchandises va s'automatiser de plus en plus, il va y avoir des pertes d'emploi parmi les chauffeurs de camion, ce qui représente une perte d'emploi très importante. Il est probable que des gens devront changer de métier et il faudra donc réfléchir à la façon d'effectuer cette transition à l'avenir.

Du point de vue de la planification commerciale, il me paraît prématuré d'en parler parce que nous pensons avoir un véhicule entièrement autonome, de niveau d'entrée 4, pour 2021. C'est un échéancier très éloigné pour la planification commerciale. Ce véhicule sera utilisé, comme je l'ai dit, dans un environnement géographiquement limité, de sorte que le premier véhicule ne sera probablement pas capable de transporter un gros volume. Ce sera plutôt un projet pilote pour que le public prenne connaissance de cette technologie, se familiarise avec elle, ce genre de chose. Les répercussions se feront probablement sentir plus tard, du point de vue de la planification commerciale, par exemple, si nous tenons compte de notre empreinte manufacturière.

[Français]

Le sénateur Cormier : Avez-vous des idées sur la façon dont le gouvernement fédéral pourrait aider la main-d'œuvre de ce secteur à prévoir ou à se préparer à cette transition et à cette transformation?

[Traduction]

M. Smith : Je suis optimiste, je crois qu'avec le temps, à mesure que les modèles commerciaux évolueront, le marché du travail perdra un certain nombre d'emplois conventionnels, mais récupérera des emplois moins conventionnels. Je ne sais pas vraiment quelle forme ils prendront. C'est sans doute un domaine que le gouvernement fédéral pourrait surveiller et il en sait certainement davantage que moi au sujet des solutions à envisager.

[Translation]

Senator Boisvenu: First of all, I would like to thank our guest. Perhaps I will finish this round of questions with a bit of philosophy.

According to the people who have appeared before our committee, the future of the automobile seems very exciting. However, my great fear concerns all these computerized systems invading our world. For example, if you lose your cell phone or access the Internet, you panic. People are losing more and more autonomy in problem-solving because they are increasingly dependent on the outside world to solve their communication problems.

We already depend on public transit; for example, if there is a blackout, the subway does not work, or airplane pilots may go on strike. We are also in a world that depends on communications, and the car depends on it as well. Humans have always sought independence in their movements, and they have always sought independence to solve problems.

We will be facing an automotive market where it will be almost impossible to do any car repairs, such as changing a belt, because everything will be computerized. Is the industry going to propose a plan B, in which we will not have to rely completely on the autonomous mode in our movements, and basically become slaves of our homes? Will there be other ways to be independent in our movements, so that we are not completely dependent on them?

This aspect frightens me a little.

[English]

Mr. Smith: I guess the move to autonomous vehicles or the penetration of autonomous vehicles into the fleet will take a significant amount of time. Only about 8 per cent of the vehicle fleet changes over in any given year, and the average vehicle on the road today in Canada is over 10 years. With both the durability of existing vehicles and how the technology flows in, they're not suddenly all going to be autonomous vehicles 10 years from now.

I view my personal mobility as very important and driving is still a pleasure, so I'm sure there are folks like me and there will continue to be a market for people who want to drive. As long as there's a market for those vehicles, we will want to supply it.

[Translation]

Senator Boisvenu: I am looking at the technologies embedded in our cars. Mine has warnings all around. If I pass someone, I get a warning. If I touch a white line, the steering wheel vibrates. Driving a vehicle, whatever kind, is a century-old practice for humans. We will no longer need our reflexes to drive our cars.

[Français]

Le sénateur Boisvenu : Je voudrais tout d'abord remercier notre invité. Je vais peut-être finir cette ronde de questions avec un peu de philosophie.

Selon les gens qui sont venus témoigner devant notre comité, l'avenir de l'automobile semble très palpitant. Cependant, ma grande crainte concerne tous ces systèmes informatisés qui envahissent notre monde. Par exemple, si on perd son téléphone cellulaire ou l'accès à Internet, on panique. L'homme perd de plus en plus d'autonomie à résoudre les problèmes, parce qu'il est de plus en plus dépendant de l'extérieur pour régler ses problèmes de communication.

Nous sommes déjà dépendants du transport en commun; par exemple, s'il y a une panne d'électricité, le métro ne fonctionne plus, ou il peut y avoir, par exemple, une grève des pilotes d'avion. Nous sommes aussi dans un monde de dépendance aux communications, et l'automobile en dépend aussi. L'homme a toujours recherché l'autonomie dans ses déplacements, et il a toujours recherché l'autonomie pour résoudre des problèmes.

Nous ferons face à un marché de l'automobile où il deviendra presque impossible de faire la moindre réparation à une voiture, par exemple, pour changer une courroie, car tout sera informatisé. Est-ce que l'industrie nous proposera un plan B selon lequel nous ne serons pas obligés de nous fier complètement au mode autonome dans nos déplacements, et de devenir esclaves de notre résidence, dans le fond? Est-ce qu'il y aura d'autres moyens d'être autonomes dans nos déplacements, afin que nous n'en soyons pas complètement dépendants?

Cet aspect m'effraie un peu.

[Traduction]

M. Smith : Je pense que l'adoption des véhicules autonomes ou l'intégration des véhicules autonomes dans les flottes de véhicule prendra un certain temps. Huit pour cent des flottes de véhicule sont renouvelés chaque année, et en moyenne, un véhicule est utilisé au Canada pendant plus de 10 ans. Compte tenu de la durabilité des véhicules existants et de l'arrivée des nouvelles technologies, il est certain que tous les véhicules ne seront pas autonomes dans 10 ans.

La mobilité personnelle est pour moi une chose très importante et conduire est toujours un plaisir pour moi; je suis donc certain qu'il y a d'autres gens comme moi et qu'il y aura toujours un marché pour les gens qui veulent conduire. Tant qu'il y aura un marché pour ces véhicules, nous allons continuer à l'approvisionner.

[Français]

Le sénateur Boisvenu : Je regarde les technologies intégrées dans nos voitures. Dans la mienne, il y a des avertisseurs tout autour. Si je fais un dépassement, on m'avertit. Si je touche à une ligne blanche, le volant vibre. Conduire un véhicule, quel qu'il soit, est une pratique centenaire pour l'humain. Nous n'aurons plus besoin de nos réflexes pour conduire notre voiture.

So I am repeating my question. In situations of total dependence, will there be alternate means that will allow humans to continue their journey? If I buy a car tomorrow and it breaks down because of the computer system, will I get stuck or will there be mechanisms in the car that will ensure that I can drive it without having to depend on the computer system?

[English]

Mr. Smith: There are several levels of automation. A vehicle that is a low level of automation, level 2 or below, if it has a system fail, may well be able to continue. It will depend on whether it involves critical safety systems. If it did have a failure of that sort of system, the vehicle would probably disable itself. But electronic failures are relatively uncommon.

With higher levels of automation, the vehicle we intend to come to market within a 2021 time frame has no steering wheel, no brakes and no gas pedal, so you would start it, in essence, launch it, more like launching your phone or your computer at the start of the day. Then you probably have to put a destination or tell it where to go or whatever, but it would take over.

I want to come back to something. Statistics say that the vast majority of fatalities come from operator error of one form or another. Some of it's distraction, some of it's substance and some of it's speed. There are all sorts of things, but it's a very high percentage. That is a safety opportunity with lives to be saved.

There is a net safety benefit to the technologies that are regulated on vehicles today. Transport Canada has been able to say we will save "X" number of lives with this technology. That's why it has come forward. Some of the newer technologies haven't quite hit the threshold where that's demonstrated yet, but certainly insurers are taking note and pushing. In the U.S., there's a voluntary agreement on automated emergency braking. We'll see what Canada does.

There is a benefit to these technologies. It's pretty clear the vehicle-to-vehicle technology, if it becomes regulated, DSRC will be coming on to vehicles because there's a net safety benefit where the system says to the vehicle you're not doing something you need to do to be safe, and it will either signal or intervene. So you can see how vehicle-to-vehicle technology could work. I've seen these sorts of displays.

A vehicle is dead in the road and a vehicle is between you and that dead vehicle. DSRC would say there's a dead vehicle up there and tell the vehicle to slow down or stop to avoid the collision. That's an intervention where the technology has stepped in and

Je répète donc ma question. Est-ce qu'il y aura, dans des situations de dépendance totale, des moyens parallèles qui permettront à l'humain de continuer à se déplacer? Si je m'achète une voiture demain et qu'elle tombe en panne à cause du système informatique, est-ce que je serai coincé ou y aura-t-il des mécanismes dans l'automobile qui feront en sorte que je pourrai la conduire sans devoir dépendre du système informatique?

[Traduction]

M. Smith : Il y a plusieurs niveaux d'automatisation. Le véhicule qui est à un faible niveau d'automatisation, le niveau 2 ou moins, peut fort bien continuer à fonctionner en cas de panne d'un système. Ça ne sera pas le cas si ce sont les systèmes de sécurité essentiels qui sont touchés. S'il y avait une panne dans ce type de système, le véhicule s'arrêterait probablement de lui-même. Mais les pannes électroniques sont relativement rares.

Lorsqu'on parle de niveaux d'automatisation plus élevés, le véhicule que nous avons l'intention de commercialiser d'ici 2021 n'aura pas de volant, pas de pédale de frein, ni d'accélérateur, de sorte que vous allez le démarrer, en fait, l'activer, comme vous le faites pour votre téléphone ou votre ordinateur le matin. Vous aurez probablement ensuite à inscrire la destination ou lui dire où il doit aller, mais c'est lui qui prendra ensuite en charge le déplacement.

J'aimerais revenir sur quelque chose. Selon les statistiques, l'immense majorité des décès vient d'une erreur de l'opérateur, sous une forme ou une autre. C'est parfois que l'opérateur a été distrait, c'est parfois un problème grave et c'est parfois la vitesse. Il y a toutes sortes de raisons, mais c'est un pourcentage très élevé. Cette technologie va donc renforcer la sécurité et épargnera des vies.

Les technologies réglementées qui sont utilisées aujourd'hui dans les véhicules offrent un grand avantage sur le plan de la sécurité. Transports Canada a été en mesure de dire que telle technologie permettra de sauver un nombre de vies défini. C'est la raison pour laquelle cette question a progressé. Les technologies les plus récentes n'ont pas encore atteint un point où cela peut être démontré, mais il est évident que les compagnies d'assurance suivent de près la situation et cherchent à faire avancer les choses. Aux États-Unis, il existe une entente volontaire sur les freins d'urgence automatisés. Nous verrons ce que fera le Canada.

Ces technologies comportent des avantages. Cela est assez clair pour la technologie de la communication entre les véhicules, si cela est réglementé, le DSRC sera intégré aux véhicules, parce qu'il y a un avantage net pour la sécurité lorsque le système peut dire au véhicule qu'il ne fait pas quelque chose qu'il doit faire pour la sécurité et ensuite, il signalera le problème, ou il interviendra. Vous pouvez donc voir comment la technologie des communications entre les véhicules pourrait fonctionner. J'ai vu des représentations de ce genre.

Un véhicule est en panne au bord de la route et il y a un véhicule qui se trouve entre vous et ce véhicule en panne. Le DSRC pourrait dire qu'il y a un véhicule en panne devant, et dire à l'autre véhicule qu'il doit ralentir ou s'arrêter pour éviter

prevented a serious consequence. That is, in fact, the kind of opportunity we're facing, and that's a relatively low level of automation. The further you automate, the bigger the opportunity.

The Chair: Colleagues, I would like to thank Mr. Smith for his participation today.

Honourable senators, for our meeting tomorrow, which will be our last meeting of the session, we will hear from the representatives of the Intelligent Transportation Systems Society of Canada.

(The committee adjourned.)

OTTAWA, Wednesday, June 14, 2017

The Standing Senate Committee on Transport and Communications met this day at 6:45 p.m., in public and in camera, for a public and in camera session to continue its study on the regulatory and technical issues related to the deployment of connected and automated vehicles.

Senator Dennis Dawson (Chair) in the chair.

[Translation]

The Chair: Honourable Senators, the Standing Senate Committee on Transport and Communications is continuing its study on the regulatory and technical issues related to the deployment of connected and automated vehicles.

[English]

I'm pleased to introduce our witness. Mr. David Michelson is Co-Chair of the Intelligent Transportation Systems Society of Canada and also a professor at the University of British Columbia.

[Translation]

Thank you for being with us this evening. I invite you to make your presentation. Then senators will ask questions.

[English]

David Michelson, Co-Chair of the Intelligent Transportation Systems Society of Canada and Professor, University of British Columbia, as an individual: You are no doubt aware and have probably heard of Arthur C. Clarke's famous observation that every revolutionary idea seems to evoke three stages of reaction. The first is it's completely impossible. The second is it's possible but it's not worth doing. Of course the third stage is, "I said it was a good idea all along." Few would disagree that connected and automated vehicle technologies are passing through stage two and are firmly on their way toward stage three.

une collision. C'est une intervention où la technologie intervient et empêche une conséquence grave. C'est en réalité le genre de possibilité qui s'offre à nous et il s'agit là d'un niveau d'automatisation relativement faible. Plus l'automatisation progresse, plus il y a de possibilités.

Le président : Chers collègues, j'aimerais remercier M. Smith d'avoir participé aujourd'hui à nos débats.

Honorables sénateurs, nous accueillerons à la séance de demain, qui sera la dernière séance de la session, des représentants de la Société des systèmes de transport intelligents du Canada.

(La séance est levée.)

OTTAWA, le mercredi 14 juin 2017

Le Comité sénatorial permanent des transports et des communications se réunit aujourd'hui, à 18 h 45, en séance publique et à huis clos, afin de poursuivre son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés.

Le sénateur Dennis Dawson (président) occupe le fauteuil.

[Français]

Le président : Honorables sénateurs et sénatrices, le Comité sénatorial permanent des transports et des communications poursuit son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés.

[Traduction]

Je suis heureux de présenter notre témoin, M. David Michelson, coprésident de la Société des systèmes de transport intelligents du Canada et professeur à l'Université de la Colombie-Britannique.

[Français]

Merci d'être avec nous ce soir. Je vous invite à faire votre présentation. Par la suite, les sénateurs vous poseront des questions.

[Traduction]

David Michelson, coprésident, Société des systèmes de transport intelligents du Canada, et professeur, Université de Colombie-Britannique, à titre personnel : Vous avez sans doute déjà entendu la fameuse remarque d'Arthur C. Clarke comme quoi chaque idée révolutionnaire semble entraîner trois phases de réaction : premièrement, que c'est complètement impossible; deuxièmement, que c'est possible, mais que cela n'en vaut pas la peine; la troisième phase étant, bien sûr, celle où on prétend avoir toujours su que c'était une bonne idée. Et il y aurait consensus, je pense, pour dire que les technologies de connectivité et d'automatisation des véhicules sont en train de franchir la deuxième phase et de parvenir à la troisième.

It's notable that it's fairly rare for emerging technologies of this sort to be greeted with as much interest and enthusiasm by such a broad cross section of society at such an early stage in their development. Perhaps it's a reflection of our collective frustration with existing modes of transportation, our faith in advanced technologies, the vast potential of connected and automated vehicle technologies to have significant impacts on an urban scale, and the ease with which the advantages of the technologies can be appreciated on a human scale. It's not difficult to imagine that Robert Moses and Jane Jacobs might both approve, although obviously for different reasons.

From your previous deliberations you're certainly familiar with the goals of connected and automated vehicle technologies, but I'll repeat them here. Simply put, we want to first of all improve road safety; second, reduce traffic congestion and minimize environmental impact; and third, enhance commercial vehicle efficiency.

But when we consider the relevant technical and regulatory challenges associated with implementing these technologies, we have to be very clear that the role of these technologies is not simply to collect, exchange or display information concerning the driving environment. It is not just about the sensors and the communications links. Instead, we can never forget their fundamental purpose is to support decision making by the driver, whether a person or a machine. Decisions can erode safety — whether to brake, steer right or left and even whether the decisions should be initiated by a man or a machine — must generally be made in fractions of a second and based on real-time data.

Decisions concerning the selection of driving routes in order to minimize trip time, tolls, fuel consumption or traffic congestion can be made over much longer time scales and in some cases based upon scant or even historical data. Even the data exchanges that comprise commercial vehicle operations ultimately revolve around decisions: Were the right data exchanged? Is the process complete?

The needs of the decision-making process ultimately set the requirements and specifications for the sensors, actuators, interfaces and communication devices that link connected and automated vehicles to their surroundings and to each other and ultimately set the technical and regulatory requirements. Both sides are important, challenging and, to this point in time, works in progress. Neither the technical side nor the decision-making side can be properly developed or indeed regulated without awareness of the limitations of the other.

While the challenges of developing products and infrastructure are quite different and must be accounted for, full appreciation of this interdependence between the technology and the decision-making processes would appear to be prerequisite for success in this field.

Soulignons au passage qu'il est assez rare que des technologies émergentes de ce type soient accueillies avec tant d'intérêt et d'enthousiasme par un si grand éventail de personnes, à un stade si précoce de leur avancement. Peut-être est-ce le reflet de la frustration collective que nous ressentons à l'égard des modes de transport existants, de notre foi dans les technologies de pointe, des répercussions majeures que pourraient avoir ces technologies sur le tissu urbain et de la facilité d'apprécier les avantages de ces technologies à une échelle humaine. On les imagine facilement suscitant l'approbation de Robert Moses et de Jane Jacobs, même si c'était pour des raisons manifestement différentes.

À l'issue de vos délibérations précédentes, vous connaissez certainement bien les objectifs des technologies de connectivité et d'automatisation des véhicules, mais je vais les répéter. Pour l'essentiel, il s'agit d'améliorer la sécurité routière, de réduire les embouteillages et de minimiser les répercussions sur l'environnement, puis d'améliorer l'efficacité des véhicules commerciaux.

Pour étudier les défis réglementaires et techniques pertinents liés à la mise en œuvre de ces technologies, il faut toutefois ne pas perdre de vue un point essentiel : que le rôle de ces technologies va plus loin que la collecte, l'échange ou l'affichage de renseignements portant sur l'environnement de conduite; il va plus loin que les capteurs et les liens de communication. Nous ne devons jamais oublier que leur objectif fondamental est d'appuyer la prise de décisions par le conducteur, qu'il s'agisse d'une personne ou d'une machine. Les décisions — freiner, donner un coup de volant à droite ou à gauche et même juger s'il faut laisser la décision à une personne ou à une machine — sont susceptibles d'éroder la sécurité et doivent généralement être prises en une fraction de seconde, à partir de données en temps réel.

Les décisions portant sur le choix des itinéraires pour minimiser la durée du trajet, les péages, la consommation de carburant ou le temps perdu dans les embouteillages peuvent requérir beaucoup plus de temps et, dans certains cas, reposer sur des données insuffisantes, voire historiques. Même les échanges de données déterminant l'exploitation de véhicules commerciaux reposent, au bout du compte, sur des décisions : les bonnes données ont-elles été échangées? Le processus est-il complet?

Ce sont, au bout du compte, les besoins du processus de prise de décisions qui déterminent les exigences et spécifications pour les capteurs, actionneurs, interfaces et appareils de communication qui relient les véhicules connectés et automatisés à leur environnement, ainsi que l'un à l'autre, déterminant ainsi, en bout de course, les exigences techniques et réglementaires. Les deux éléments sont importants, difficiles et, à l'heure où nous nous parlons, encore en cours d'élaboration. Ni l'aspect technique ni celui de la prise de décisions ne peut être élaboré correctement, ou d'ailleurs réglementé, sans tenir compte des limites de l'autre aspect.

Les défis d'élaborer des produits et de mettre en place une infrastructure sont très différents et il faut en tenir compte. Mais je dirais que le succès dans ce domaine dépend d'une véritable confiance en l'interdépendance entre la technologie et les processus de prise de décisions.

Are there important Canadian issues that remain to be addressed by these technologies? One example is that connected and automated vehicle technologies were originally conceived as a method for improving safety and reducing congestion on highways and freeways. But as the concepts have evolved over the last decade or so, their application to a greater range of driving scenarios throughout urban areas have increased. Yet, resource roads remain beyond the reach of conventional connected vehicle technology. In British Columbia alone, over 620,000 kilometres of resource roads serve the natural resources sector, remote communities and recreational sites. British Columbia is notable in that the resource roads are actually greater in extent than the conventional urban and public roads.

FPInnovations, the Canadian forest industry's national research and development organization, is embarking on an ambitious program to develop what they refer to as an intelligent forestry transportation system architecture for Canada that will build upon existing connected vehicle technologies but will reflect the realities of serving a low density of industrial users in a challenging physical environment. It's notable that unlike other groups in the natural resources sector, they are choosing to base their development on existing connected vehicle technologies rather than develop their own, which I believe is exactly the right course to take.

In addition to introducing several new service packages that reflect the data exchange and transfer needs of specific user scenarios, such systems will likely incorporate specialized networking protocols that will account for the low density of users and relative sparsity of links, as well as use dual-band radios that are compatible with urban systems but can also address the harsher propagation environment encountered in resource environments.

Whether Canadians will contribute to and benefit from connected automated vehicle technologies in some way is not in doubt. We will. Many government, industry and university groups across the country are pursuing development of various aspects of these technologies, often in collaboration with international partners, particularly in the United States. Organizations such as ITS Canada play a key role in bringing these groups together on neutral ground, where information can be exchanged seamlessly and easily. However, the full benefits of efforts in this field will only accrue to Canada if a coordinated national strategy is developed that will ensure that the best practices are shared, solutions appropriate to the Canadian condition are developed and deployed, and progress is swift.

The Chair: Thank you.

Compared to the U.S., how would you say we are progressing in being *à l'avant-garde*, in being ahead of the innovation?

Reste-t-il des questions canadiennes importantes que les technologies n'abordent pas encore? J'en aurais un exemple. Les technologies de connexion et d'automatisation des véhicules ont été conçues au départ pour améliorer la sécurité et réduire les embouteillages sur les routes et autoroutes. De plus, au cours de la dernière décennie, les concepts ont évolué et s'appliquent à une plus grande gamme de scénarios de conduite partout dans les zones urbaines. Toutefois, la technologie conventionnelle des véhicules connectés laisse à l'écart les routes de transport des ressources. Or, en Colombie-Britannique seulement, cela représente plus de 620 000 kilomètres de routes qui desservent le secteur des ressources naturelles, les collectivités éloignées et les sites de loisirs. En fait, le réseau des routes de transport des ressources de Colombie-Britannique est plus étendu que celui des routes publiques et urbaines.

FP Innovation, l'organisation nationale de recherche et développement de l'industrie forestière canadienne, entreprend un ambitieux programme visant à développer ce qu'on appelle un réseau de transport forestier intelligent pour le Canada qui s'appuie sur les technologies de véhicules connectés actuelles, mais qui tient compte de la réalité des utilisateurs industriels peu nombreux situés dans un environnement difficile. Contrairement à d'autres groupes du secteur des ressources naturelles, le secteur forestier choisit de fonder son développement sur les technologies de véhicules connectés actuelles au lieu de développer sa propre technologie. Je crois que c'est exactement l'approche qu'il convient d'adopter.

En plus d'offrir plusieurs nouveaux services qui s'adressent aux besoins particuliers des utilisateurs en matière d'échange et de transfert de données, ces systèmes vont sans doute comprendre des protocoles de réseautage spécialisés pour les utilisateurs dans les régions à faible densité où les réseaux de communications se font rares. Ces systèmes vont également employer des radios double bande compatibles avec les réseaux urbains, mais qui réagissent mieux dans des milieux où la propagation des ondes est plus difficile, comme on le voit dans le secteur des ressources naturelles.

Il ne fait aucun doute que les Canadiens vont contribuer à l'évolution des technologies liées aux véhicules connectés et automatisés, et qu'ils vont profiter de ces technologies. Bien des gouvernements, des entreprises et des universités au pays cherchent à améliorer divers aspects de ces technologies, souvent en collaboration avec des partenaires internationaux comme les États-Unis. Les organisations comme la Société des systèmes de transports intelligents du Canada jouent un rôle clé afin que ces groupes travaillent sur un pied d'égalité, afin que les renseignements puissent être communiqués facilement. Toutefois, le Canada ne pourra profiter de ces efforts que si une stratégie nationale coordonnée permet d'appliquer les pratiques exemplaires, d'apporter des solutions adaptées aux conditions canadiennes ainsi que de faire des progrès rapides.

Le président : Merci.

Comparativement aux États-Unis, êtes-vous d'avis que nous faisons des progrès afin d'être à l'avant-garde en matière d'innovation?

Mr. Michelson: I would say we're catching up. It certainly is notable that the DSRC spectrum that has been allocated for use in the United States for over 10 years is not yet allocated in Canada. Anyone who wants to experiment with connected vehicle technology has to get a developmental licence from Innovation, Science and Economic Development Canada. They can't just install the equipment and use it directly, as they would in the U.S. This is actually a bit of an impediment to development and innovation.

The Chair: It's done on a one-on-one basis. They have to individually ask. Because, in the States now, people apply the technology. Here, we have to apply for it.

Mr. Michelson: Yes, we have to apply for a special developmental licence. It's a fairly intensive application to prepare, and it takes a long time to approve. My colleagues at the University of Alberta applied for a developmental licence, and it took several months for them to get permission and approval, which was a bit of a surprise. So this is one regulatory issue that is holding things up. Of course, I said it's moving very quickly now to move towards allocating, not just reserving, the spectrum. Once that happens, things will be a lot easier. We certainly hope it will be sooner rather than later.

Senator Bovey: We have been really intrigued with all we have heard over these past months. Thank you for your contribution today. I was intrigued that you talk about a national strategy and best practices, and that ties in, of course, to regulations.

I have two questions. The first is: Who leads that? We've talked to various parts of the sector, and it seems to me that there are great minds working in many dimensions in the field. How does it come together as a national strategy rather than the pieces of the puzzle?

Mr. Michelson: Those are very good questions.

Within the federal government, there are three organizations that are striving to contribute and assume leadership. We know that the National Research Council, for example, just last week held a special meeting that brought together people from various government and other agencies to outline their strategy for trying to push for a unified effort within Canada.

Of course, our friends at Transport Canada have also been pushing forward in this area for a long time, although they did have an intelligent transportation systems group until a few years ago. That was disbanded. The ITS activity was then dispersed within the organization.

We're very glad to hear that our friends at Innovation, Science and Economic Development Canada, in spectrum management, are also pushing forward now. They've issued a couple of bulletins during the last several months indicating that they are

M. Michelson : Je dirais que nous rattrapons notre retard. Je signale que le spectre de communication spécialisé à courte portée qu'on peut utiliser aux États-Unis depuis plus de 10 ans n'est toujours pas accessible au Canada. Toute entreprise qui veut mettre à l'essai une technologie de véhicules connectés doit obtenir un permis de développement octroyé par le ministère de l'Innovation, des Sciences et du Développement économique. On ne peut pas simplement installer l'équipement et l'utiliser directement comme aux États-Unis. C'est d'ailleurs un obstacle qui freine le développement et l'innovation.

Le président : Les permis sont accordés au cas par cas. Chaque entreprise doit présenter sa propre demande. Aux États-Unis, on peut directement appliquer la technologie, tandis qu'au Canada, il faut présenter une demande.

M. Michelson : Oui, les entreprises canadiennes doivent demander un permis spécial de développement. Le processus d'approbation est assez exigeant et requiert beaucoup de temps. Mes collègues de l'Université de l'Alberta ont dû attendre plusieurs mois avant d'obtenir leur permis de développement. Ces délais, qui ont causé une certaine surprise, constituent un obstacle réglementaire qui ralentit l'innovation. Cependant, je répète que nous réalisons des progrès rapides vers l'attribution des fréquences, et non seulement leur réservation. Lorsque cette attribution deviendra réalité, tout sera beaucoup plus facile. Nous espérons que cette attribution pourra se faire bientôt.

La sénatrice Bovey : Les témoignages entendus ces derniers mois nous ont vivement interpellés. Je vous remercie de votre contribution aujourd'hui. J'ai été intriguée que vous parliez d'une stratégie nationale et de pratiques exemplaires qui sont, bien sûr, liées à la réglementation.

J'ai deux questions. Tout d'abord, qui serait le chef de file? Nous avons parlé avec divers intervenants du secteur, et il semble que de grands spécialistes soient à pied d'œuvre pour bien des aspects du domaine. Comment peut-on en arriver à une stratégie nationale où tout le monde travaille de concert, au lieu d'avoir une mosaïque d'efforts disparates?

M. Michelson : Il s'agit de très bonnes questions.

Au sein du gouvernement fédéral, il y a trois organismes qui font une contribution et assument le leadership. Nous savons que le Conseil national de recherches, par exemple, a tenu une réunion spéciale la semaine dernière qui réunissait des gens de divers organismes gouvernementaux et autres pour énoncer leur stratégie d'unification des efforts au Canada.

Évidemment, nos collègues de Transports Canada font aussi des progrès dans ce domaine depuis longtemps, même s'ils avaient un groupe de systèmes de transport intelligents jusqu'à il y a quelques années. Il a été démantelé. Les activités des STI ont ensuite été réparties au sein de l'organisation.

Nous sommes très heureux d'entendre que nos amis à Innovation, Sciences et Développement économique Canada chargés de la gestion du spectre font aussi désormais des progrès. Au cours des derniers mois, ils ont émis quelques bulletins indiquant

moving forward with the process of coming up with regulations for technical specifications for vehicle-to-vehicle onboard units, et cetera. So many groups are working but the strategy seems to be very informal at this point. We'd certainly welcome a more formal strategy.

Senator Bovey: One part of it, of course, is infrastructure, right?

Mr. Michelson: Absolutely.

Senator Bovey: Where should the funding for infrastructure come from?

Mr. Michelson: That's a very good question. It's certainly what is holding things up.

It's notable that in the United States, the Department of Transportation purposely left out infrastructure in their initial forays into the strategy by focusing on vehicle-to-vehicle communications, where relatively inexpensive units, onboard units, or after-market safety devices could be deployed within vehicles and achieve most of their goals.

So the infrastructure costs are huge in terms of both the expense of the equipment and the expense of installing them and even the cost of the radio licences. If you're installing lots and lots of equipment, the cost of radio licences can add up quickly.

Senator Bovey: On the work you did with the City of Toronto, which I believe your organization did, I wonder if you could elaborate on the initiative you took there.

Mr. Michelson: I wasn't personally involved in the work with Toronto, so I can't comment on that, unfortunately.

Senator Bovey: Okay. Thank you.

Senator MacDonald: Thank you, Mr. Michelson, for being here.

You're with the University of British Columbia. On the website, it says that you've been working alongside a Vancouver-based startup, Moovee Innovations. Moovee Innovations suggests that ITS can offer a solution to traffic gridlock, a problem it believes will be magnified by retiring Baby Boomers' driving impairments. I wonder if you could elaborate on that, exactly what sort of work you have been doing with them and how you see it being applied in the next decade.

Mr. Michelson: We're not doing as much work with them now. We were working with them about a year ago. So that information is slightly outdated, but Moovee continues to work on their concepts. Most of these automated-vehicle concepts are based on bringing together three technologies. Usually, one group will work on the drive train, the electric vehicle component. One

qu'ils allaient de l'avant avec un processus de rédaction de réglementation pour les spécifications techniques des unités embarquées entre véhicules, et cetera. De nombreux groupes travaillent à la stratégie, qui semble toutefois très officielle pour l'instant. Nous accueillerions certainement une stratégie plus officielle.

La sénatrice Bovey : L'une des composantes est évidemment l'infrastructure, n'est-ce pas?

M. Michelson : Absolument.

La sénatrice Bovey : D'où devrait provenir le financement pour les infrastructures?

M. Michelson : C'est une très bonne question. C'est certainement un facteur qui a ralenti les progrès.

Notons qu'aux États-Unis, le département des Transports a intentionnellement laissé de côté la question des infrastructures dans sa stratégie initiale en mettant plutôt l'accent sur les communications entre véhicules, afin que des unités relativement peu coûteuses, des unités embarquées ou des dispositifs de sécurité après fabrication soient déployées dans les véhicules, ce qui leur permettait d'atteindre la plupart de leurs objectifs.

Les coûts d'infrastructure sont donc énormes en matière de dépenses et d'équipements ainsi que de coûts d'installation et de coûts de licences radio. Si on installe beaucoup d'équipements, le coût des licences radio peut augmenter rapidement.

La sénatrice Bovey : Je crois que votre organisme a travaillé auprès de la ville de Toronto. Pouvez-vous nous en dire plus sur le travail que vous y avez fait?

M. Michelson : Je n'ai pas personnellement participé aux travaux à Toronto, alors je ne peux malheureusement pas faire de commentaires.

La sénatrice Bovey : D'accord. Merci.

Le sénateur MacDonald : Merci beaucoup, monsieur Michelson, d'être ici.

Vous êtes affilié à l'Université de la Colombie-Britannique. Sur le site web, on dit que vous avez travaillé avec une jeune entreprise de Vancouver, Moovee Innovations. Moovee Innovations estime que les STI peuvent offrir une solution aux embouteillages, problème qui, semble-t-il, sera amplifié par les facultés réduites au volant des baby-boomers à la retraite. Je me demande si vous pouviez nous donner plus de détails à ce sujet. Pouvez-vous nous dire exactement ce que vous faites avec cette entreprise et comment vous voyez l'application de cette solution au cours de la prochaine décennie.

M. Michelson : Nous ne faisons plus beaucoup de travail avec cette entreprise. Nous travaillions avec elle il y a environ un an. Cette information est donc légèrement désuète, mais Moovee continue de travailler à ses concepts. La plupart de ces concepts de véhicules automatisés sont fondés sur le recours à trois technologies. Habituellement, un groupe travaille au groupe motopropulseur, les

group will work on the software that actually takes care of doing the routing and the assignment and the oversight, and then one group will work on the communications technology.

Moovee is pushing on the communication technology. Their founder has a great background in the Canadian telecommunications industry. It is basically providing transportation as a service on demand, and they believe that, by having the correct communications infrastructure and software in place, they can get vehicles to where they are needed quickly. That's really what Moovee's concept is all about, combining that with a lightweight, relatively inexpensive vehicle. It's dispatch services that Moovee is really pushing.

Senator MacDonald: Where do they get their capital? Where does the funding come from?

Mr. Michelson: The founder of Moovee Innovations spends a lot of his time looking for venture capital. He has been looking all over the world, not just within Canada. He has been looking in the United States and, in particular, in East Asia. That's mostly where he has been looking for his support.

Senator MacDonald: What is your assessment of their work and what they are doing? How do you assess their progress?

Mr. Michelson: I think it's inevitable that someone is going to succeed in this space. But there is a lot of competition, and locating funding and capital is a big challenge for all companies in this area because there are so many people going after the same funding.

Senator Beyak: I was struck by you talking about the 620,000 kilometres of access roads as opposed to regular highways in British Columbia. I live in a part of northwestern Ontario that is very remote as well. You mentioned that the only way it's going to work, urban and rural, is if there is a coordinated national strategy. I am wondering if you know of anyone who is putting together something like that at the federal level now, or if our committee could recommend some sort of an initiative. I think the urban-rural divide is going to be huge on this issue down the road.

Mr. Michelson: Absolutely. That was one of the reasons why, when FPInnovations approached me, I jumped at the opportunity because I see the same opportunity that you do. They have a very good relationship with Transport Canada, which is good.

We're hoping that once we get our proposal together — we're evaluating; we are also talking with ISED about some of the spectrum-management issues, allocation of spectrum at UHF. We're hoping this will work out. Everyone seems to be very receptive and has been very helpful, but encouragement from this committee would no doubt help, knowing that this is something that would be good for Canada.

composantes électriques du véhicule. Un groupe travaille au logiciel qui s'occupe du routage, de l'assignation et de la surveillance, puis un groupe travaille à la technologie de communications.

Moovee se concentre sur la technologie de communications. Son fondateur a une grande expérience de l'industrie canadienne des télécommunications. L'entreprise offre essentiellement le transport comme un service sur demande, et elle croit que, en ayant les bonnes infrastructures de communications et les bons logiciels, elle peut faire circuler les véhicules rapidement. Voilà ce en quoi consiste le concept de Moovee, lequel peut être appliqué à un véhicule léger relativement peu coûteux. Moovee met en fait l'accent sur les services de répartition.

Le sénateur MacDonald : Où vont-ils chercher leurs capitaux? D'où vient leur financement?

M. Michelson : Le fondateur de Moovee Innovations passe une bonne partie de son temps à rechercher du capital-risque. Il cherche partout dans le monde, pas uniquement au Canada. Il cherche également aux États-Unis et, plus particulièrement, en Asie de l'Est. C'est principalement là-bas qu'il cherche son appui.

Le sénateur MacDonald : Comment trouvez-vous leurs activités et ce qu'ils font? Trouvez-vous qu'ils font des progrès?

M. Michelson : Je crois qu'il est inévitable que quelqu'un réussisse dans ce secteur. Mais il y a beaucoup de concurrence et il est très difficile de trouver des fonds et des capitaux pour toutes les compagnies dans ce secteur, car il y a bien des gens qui sont en lice pour le même financement.

La sénatrice Beyak : J'ai été frappée de vous entendre parler de 620 000 kilomètres de route d'accès par opposition aux autoroutes habituelles en Colombie-Britannique. J'habite dans une partie du Nord-Ouest de l'Ontario qui est très éloignée également. Vous avez dit que la seule façon dont cela va pouvoir fonctionner, en région urbaine comme rurale, sera d'avoir une stratégie nationale coordonnée. Je me demande si vous connaissez quelqu'un qui travaille actuellement à quelque chose de semblable à l'échelle fédérale ou si votre comité pourrait nous recommander un genre d'initiative. Je crois que le fossé entre les régions urbaines et rurales sera énorme à ce chapitre, à l'avenir.

M. Michelson : Absolument. C'est une des raisons pour lesquelles lorsque le personnel de FPInnovations a pris contact avec moi, j'ai sauté sur l'occasion, car j'y vois le même potentiel que vous. Ils ont une très bonne relation avec Transports Canada, ce qui est une bonne chose.

Nous espérons qu'une fois que notre proposition sera prête — en fait nous sommes en train d'évaluer les choses; nous sommes également en pourparlers avec ISDE Canada pour ce qui est de certaines des questions de gestion du spectre, de l'allocation du spectre à ultra haute fréquence. Nous espérons que cela va fonctionner. Tout le monde semble très ouvert face à cette idée et a été très utile, mais que ce comité nous encourage serait sans aucun doute positif, sachant que c'est quelque chose qui serait bon pour le Canada.

Senator Eggleton: Thank you for your presentation. I was amused by the reference to Robert Moses and Jane Jacobs. I'm familiar with that reference and the battles pursued there.

Tonight we're introducing the phrase "intelligent transportation systems," IDS, which aside from being the name of your organization is also a system or systems. We have been using automated vehicles, EVs, or connected vehicles, CVs, and various derivatives of that in terms of vehicle-to-infrastructure and vehicle-to-vehicle. What is the difference between "intelligent transportation systems" and those other terms?

Mr. Michelson: The concept came up about 20 years ago. It was originally called "intelligent vehicle and highway information systems." This is a U.S. Department of Transportation concept. Originally it was applied mostly to freeways and highways where it was felt there was a need to automate some of the processes required to reduce traffic congestion, et cetera, on freeways. We still see in some American cities traffic lights that limit access to on-ramps, et cetera, so they wanted to go to the next step forward and actually have wireless devices on vehicles as well.

So this evolved into a concept called "intelligent transportation systems," which they thought was broader. It was applied to more than just highways. It applied to all public roads, including urban areas. ITS basically refers to the entire urban system, which includes the infrastructure as well as the vehicles.

Within ITS, you have traffic management systems, communication and infrastructure systems, and vehicles. Those are the three major components.

Senator Eggleton: You made reference to costly infrastructure in answer to the previous question from Senator Bovey. We have also had people here who have said that the industry itself should be able to absorb the infrastructure costs. Do you not see that as a possibility? Is it going to be municipal or local government that will have to absorb infrastructure costs to accommodate automated and connected vehicles?

Mr. Michelson: The infrastructure costs associated with commercial vehicle operations can almost certainly be absorbed by existing budgets and processes. Basically it will replace a lot of systems currently used but probably much more inexpensively and effectively. There is a good case for commercial vehicle operations and there isn't a big funding issue. It's mostly a matter of managing the transition from existing RFID systems to the more capable DSRC based systems.

When it comes to safety in terms of vehicle-to-vehicle communications, the cost of deploying the equipment per vehicle is \$150, so it's not very expensive. That can be absorbed

Le sénateur Eggleton : Merci pour votre exposé. J'ai été amusé par votre allusion à Robert Moses et à Jane Jacobs. Je suis au courant de leur histoire et des batailles qu'ils se sont livrées.

Ce soir, nous présentons l'expression « systèmes de transport intelligent », ou STI, qui en plus d'être le nom de votre organisation, est également un système ou des systèmes. Nous nous servons de véhicules automatisés ou de véhicules connectés et de diverses applications, notamment de véhicule à véhicule et de véhicule à infrastructure. Quelle est la différence entre les « systèmes de transport intelligent » et ces autres termes?

M. Michelson : Le concept remonte à il y a environ 20 ans. Au départ, cela s'appelait « *intelligent vehicle and highway information systems* » ou, si vous préférez, « système intelligent de régulation de la circulation sur les autoroutes ». Il s'agit d'un concept du département américain des Transports. À l'origine, on s'en servait surtout sur les autoroutes, où l'on estimait qu'il fallait automatiser certains des processus visant à réduire la congestion, notamment sur les autoroutes. Dans certaines villes américaines, on voit encore des feux de signalisation qui limitent l'accès aux bretelles d'autoroute, notamment, alors ils ont voulu pousser plus loin et avoir également des dispositifs sans fil sur les véhicules.

Cela a donc évolué pour devenir le concept qu'on a baptisé « systèmes de transport intelligent » qui, selon eux, était plus large. On ne l'a pas simplement appliqué aux autoroutes, mais bien à toutes les routes du réseau public, y compris dans les zones urbaines. Les STI couvrent en fait la totalité du réseau urbain, ce qui inclut l'infrastructure ainsi que les véhicules.

Au sein des STI, vous avez des systèmes de gestion de la circulation, des systèmes de communication et d'infrastructure et des véhicules. Voilà les trois principales composantes.

Le sénateur Eggleton : En répondant à la précédente question de la sénatrice Bovey, vous avez mentionné des infrastructures coûteuses. Nous avons également reçu des témoins qui nous ont dit que l'industrie elle-même devrait pouvoir absorber les coûts de l'infrastructure. Ne pensez-vous pas que ce serait possible? Faudra-t-il que ce soit l'administration municipale ou locale qui absorbe les coûts d'infrastructure pour recevoir des véhicules automatisés et connectés?

M. Michelson : Les coûts en infrastructure associés à l'utilisation des véhicules commerciaux peuvent très certainement être absorbés par les budgets et les processus en place. Essentiellement, cela remplacera bon nombre de systèmes qui sont présentement utilisés, mais de façon probablement beaucoup moins coûteuse et beaucoup plus efficace. Il y a lieu de plaider en faveur de l'utilisation des véhicules commerciaux et il n'y a pas de gros problèmes de financement. C'est avant tout une question de gestion de la transition des systèmes RFID actuels aux systèmes de CDCP qui sont plus efficaces.

En ce qui a trait à la sécurité sur le plan des communications de véhicule à véhicule, le coût associé au déploiement de l'équipement par véhicule est de 150 \$. Ce n'est donc pas très

into the cost of the vehicle very easily. Even for after-market devices, which they refer to as “after-market safety devices,” the cost is quite reasonable.

The main cost is if you're talking about putting all the DSRC equipment on things like traffic lights, pedestrian push buttons and the various ITS equipment associated with traffic signalling. That's where the real expense is going to be. That's why people have backed off a bit in terms of recommending all the stuff be deployed.

It's hard to see that the only group that is going to be able to absorb that will be municipal government or at least pay for that directly. They would probably need assistance from federal government and elsewhere.

Senator Eggleton: There is also a timing aspect to this. You give the reasons, which we have heard before, of improved road safety, reduced traffic congestion, minimized environmental impact and enhanced commercial vehicle efficiency. But that's not all going to happen suddenly. It's going to happen over two or three decades maybe. There is going to be a lot of co-existence between more automated vehicles and existing kinds of vehicles on the road, so at what stage does government have to look at infrastructure needs and make those kinds of changes? Making changes for just a few vehicles, which might be the case in the early stages that are requiring that kind of infrastructure, would be rather expensive and not seem to be very popular, if in fact there are very few vehicles in the early stages that would require it.

Mr. Michelson: In my personal opinion, I think that if we focused on commercial vehicle operations because there are not as many vehicles used for transfer of freight and goods — they are mostly involved in things like intermodal transport points, freight terminals and border crossings — that would be the logical place to deploy stuff first. There are already budgets in place to absorb the cost of infrastructure. There is a definite commercial advantage because it would speed up processes and the checking of freight manifests at these sites and would be a good place to get some early experience.

That's what I would tend to recommend, although it's interesting that the U.S. Department of Transportation is taking the opposite route. They are wanting to focus on V2V and road safety. That's a little bit harder in some ways because, as you say, so many vehicles have to be equipped. It's taking Robert Metcalfe's observation of the value of a network is a proportional number of nodes and networks squared. I think in this case it's probably a far higher exponent than that, so it would have to be universally mandated.

You could approach it from either side. I think the commercial vehicle operation side is one that needs to be looked at a lot more seriously. I have heard from people who actually operate this equipment that existing, active RFID systems are not as reliable

coûteux. Cela peut très bien être absorbé dans le coût du véhicule. Même pour ce qui est des dispositifs de seconde monte, que l'on appelle « dispositifs de sécurité de seconde monte », le coût est plutôt raisonnable.

La majeure partie du coût aurait à voir avec le fait d'installer tout l'équipement de CDCP sur des choses comme les feux de circulation, les boutons pour le passage des piétons et les différents appareils STI associés à la signalisation de la circulation. C'est là qu'il y aura de vraies dépenses. Cela explique pourquoi les gens se sont abstenus de recommander que toutes ces choses soient déployées.

Il est difficile de voir que le seul groupe qui sera en mesure d'absorber ce coût, ou du moins de payer pour cela directement, sera l'administration municipale. Elle aura probablement besoin de l'aide du gouvernement fédéral et d'autres sources.

Le sénateur Eggleton : Il y a aussi le volet échéancier. Vous nous avez déjà parlé des raisons suivantes : une plus grande sécurité routière, une réduction de la congestion, une réduction de l'incidence négative sur l'environnement et une plus grande efficacité des véhicules commerciaux. Toutefois, tout cela n'arrivera pas subitement. Cela se fera sur 20 ans ou peut-être 30 ans. Sur les routes, il y aura une grande coexistence entre un nombre accru de véhicules automatisés et les genres de véhicules existants. En conséquence, à quelle étape le gouvernement devra-t-il se pencher sur les besoins en infrastructure et apporter ces types de changements? Apporter des changements pour seulement quelques véhicules — ce qui pourrait être le cas lors des premières phases qui nécessitent ce genre d'infrastructure — coûterait assez cher et ne serait pas très populaire, si, en effet, il n'y a que très peu de véhicules qui en auraient besoin au début.

M. Michelson : À mon avis, je pense que nous devrions logiquement nous intéresser aux opérations des véhicules utilitaires, car il n'y a pas autant de véhicules qui sont utilisés pour le transport de marchandises et de biens — ils servent surtout au transport multimodal, dans les gares de marchandises et aux postes frontaliers. Il existe déjà des budgets pour couvrir le coût de l'infrastructure. Cela procurerait des avantages commerciaux très nets puisque cela accélérerait les processus et la vérification des manifests du fret et ce serait l'endroit idéal pour prendre de l'expérience.

C'est ce que je recommande, quoiqu'il soit intéressant de savoir que le département des Transports américain a opté pour une autre voie. Il veut mettre l'accent sur les applications de véhicule à véhicule et la sécurité routière. D'une certaine façon, c'est plus difficile, car, comme vous le dites, il y a tellement de véhicules à équiper. Comme le disait Robert Metcalfe : « L'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs. » En l'occurrence, je pense que la puissance serait beaucoup plus élevée et il faudrait donc que ce soit imposé universellement.

L'une ou l'autre voie est envisageable. Je pense que les opérations des véhicules utilitaires constituent l'aspect qui doit être examiné beaucoup plus sérieusement. Les personnes qui utilisent l'équipement qui existe déjà ont dit que les systèmes

or easy to maintain as people would like. I think there is enough dissatisfaction with existing systems that people might look for a more capable universal system, but it would have to be one that both the U.S. and Canada would have to agree to be used as the standard for intermodal transfers and border crossings and such.

Senator Eggleton: Thank you.

[*Translation*]

Senator Boisvenu: Thank you for your presentation. I would like to make a remark, and you can tell me if I'm mistaken. Forecasters are telling us that automated vehicles will solve all sorts of problems, particularly those related to traffic. We know that Montreal has many traffic jams on the week-end.

Isn't this all a bit fanciful? In the 1970s, we said that in the year 2000 no one would have to work and we would live in a leisure society. We even thought that cars would fly. So when you say that automated vehicles will reduce road traffic, isn't this a bit of a stretch of the imagination, in your opinion?

[*English*]

Mr. Michelson: It's actually very interesting. When one looks at how technology evolves, it doesn't happen in a straight line. People often have an idea about something that could be possible and will try it out. They will run into problems and have to back off. Then sometime later, new technology will come along and simplify things.

A classic example would be the case of Telidon, which many people in this room may remember from the early 1980s. The Government of Canada put a lot of money into it. It was developed right here in Ottawa in the communications research centre. It was a commercial failure. It didn't work out. It was too expensive. People were not willing to pay for dedicated communications links and the terminals themselves were not quite adequate, but it was a good idea. The technologies didn't exist at that time to push through the idea. I know many of the people who worked in Telidon were disappointed 15 years later when all of a sudden the World Wide Web became popular. They said, "Why is everyone so excited about this? We were working on it 15 years ago." What had happened was that the Internet had been developed and this was a layer on top of the Internet, and that made it commercially viable.

I suspect the same thing here. The idea for Telidon was good, but it was just that the underlying supporting technologies had not quite been developed. I think many people are sensing now that the underlying technologies that were needed were not available in 1970s, 1980s or 1990s. But they may become available now and I think that's why people are hopeful. It may be, as you say, that we won't see this in the next 10 years. There may be

RFID actifs ne sont pas aussi fiables ni aussi faciles à entretenir que les gens le souhaiteraient. Le mécontentement à l'égard des systèmes actuels est suffisamment grand pour que les gens cherchent éventuellement un système universel plus efficace, mais il faudrait que les États-Unis et le Canada s'entendent sur un système qui deviendra la norme pour le transport intermodal, les postes frontaliers, et cetera.

Le sénateur Eggleton : Merci.

[*Français*]

Le sénateur Boisvenu : Je vous remercie beaucoup de votre témoignage. Je vais vous faire part d'un constat, et vous me direz si j'ai tort. Les prévisionnistes actuels nous disent que la voiture automatisée va régler toutes sortes de problèmes, notamment ceux de la circulation. On sait que Montréal souffre énormément de la congestion routière le week-end.

Ne sommes-nous pas dans l'ordre de l'imaginaire? Au cours des années 1970, on disait qu'en l'an 2000 on serait libéré du travail et qu'on vivrait dans une société de loisirs. On croyait même que nos voitures pourraient voler. Lorsqu'on prête aux voitures automatisées cette prétention de réduire le trafic sur les routes, ne sommes-nous pas alors un peu dans la fabulation, selon vous?

[*Traduction*]

M. Michelson : En fait, c'est très intéressant. La technologie n'évolue pas de manière linéaire. Souvent, les gens imaginent quelque chose qui serait possible et essaient. Ils se butent à des obstacles et y renoncent. Puis, plus tard, arrive une nouvelle technologie qui simplifie les choses.

L'exemple classique est celui de Telidon, au début des années 1980. Vous serez nombreux à vous en souvenir. Le gouvernement du Canada y a investi beaucoup d'argent. Il a été mis au point ici même à Ottawa au Centre de recherche sur les communications. Cela a été un échec sur le plan commercial. Cela n'a pas marché. C'était trop cher. Les gens n'étaient pas prêts à payer pour des lignes de communication spécialisées et les terminaux n'étaient pas tout à fait à la hauteur, mais l'idée était bonne. À cette époque, la technologie qu'il aurait fallu pour développer cette idée n'existait pas. Je connais bien des gens qui ont travaillé au projet Telidon et qui ont été bien déçus de la popularité soudaine du World Wide Web 15 ans plus tard. Ils se sont demandé : « Pourquoi est-ce que tout le monde est si excité? On y travaillait il y a 15 ans. » Ce qui est arrivé, c'est que l'Internet s'était développé et que c'était un niveau qui se superposait à l'Internet en le rendant viable sur le plan commercial.

Je soupçonne que la même chose va se produire dans les transports. L'idée de Telidon était bonne, mais les technologies nécessaires n'avaient pas encore été mises au point. Je pense que bien des gens se rendent compte maintenant que les technologies nécessaires n'étaient pas disponibles dans les années 1970, 1980 ou 1990. Or, elles pourraient l'être maintenant et je pense que c'est pour cette raison que les gens ont de l'espoir. Comme

a road block and people may say, “This is as far as we can go and we may have to wait for 10 or 20 years.” But I think most people regard this as inevitable. Will it happen necessarily in the next 10 years? I don’t know. Your objections and concerns are quite valid. But it will happen inevitably, and it could happen sooner than we think.

Another classic example is what happened in the 1980s with cellphones and personal computers.

I will use cellphones as an example. How did people like Craig McCaw become so wealthy in the United States? Because nobody wanted cellphone licences. AT&T in 1984 or 1985 received advice from one of the largest consulting firms of the United States, McKinsey, who told them that AT&T had the opportunity to become the second carrier for cellphone service in the entire United States. They gave up that possibility because they were advised that there was only a limited number of people who would want to use cellphones, which were expensive at that time.

They said, “This is size of the market,” and AT&T said, “There’s no point in our investing in this; we can’t deal with a market this small.” Twelve years later, AT&T spent \$12 billion buying out McCaw Cellular in order to get into the cellphone business.

Our limited imagination can sometimes mean we just don’t see the possibilities until it’s too late. That was half the reason we had the tech revolution in the 1990s. Nobody wanted to get left behind again after watching the personal computer revolution. But why didn’t Hewlett-Packard want to invest in what Steve Wozniak was doing? They looked at these microcomputers he was working on and said, “These things are toys. They will not satisfy our customers.”

They were right. They were toys. They were not capable of satisfying the requirements of their enduring customers. But they didn’t realize these were disruptive technologies. They were going to improve so fast that they would overtake existing technologies.

That’s really the question that has to be asked here: How fast can these technologies improve? That’s what will make them disruptive. There are a lot of indications that now we’ve reached a critical point where sensor, software, and communications technology has reached a point where things that were not viable before may be viable now. It’s certainly worth looking at.

[Translation]

Senator Boisvenu: My next question has to do with the social aspect of the situation. Over the past 20 years, we have witnessed the widespread integration of technology in production processes. As a result, many workers have found themselves joining the

vous le dites, cela ne se fera peut-être pas au cours des 10 prochaines années. Il y aura peut-être une embûche qui fera dire aux gens : « Nous ne pouvons pas aller plus loin et il nous faudra peut-être attendre 10 ou 20 ans. » Mais je pense que la plupart des gens considèrent que c’est inévitable. Est-ce que cela va se produire nécessairement au cours des 10 prochaines années? Je ne sais pas. Vos objections et préoccupations sont tout à fait fondées. Mais c’est inévitable et cela pourrait même se produire plus rapidement que nous ne le pensons.

Autre exemple classique : ce qui est arrivé dans les années 1980 avec les téléphones cellulaires et les ordinateurs personnels.

Prenons l’exemple des téléphones cellulaires. Comment des gens comme Craig McCaw sont-ils devenus aussi riches aux États-Unis? Parce que personne ne voulait de licences de services cellulaires. En 1984 ou 1985, la plus grande entreprise de consultants des États-Unis, McKinsey, a conseillé à AT&T de devenir le deuxième fournisseur de services cellulaires aux États-Unis. AT&T n’a pas saisi cette occasion parce qu’on lui avait dit que seul un nombre limité de personnes voudraient se servir de téléphones cellulaires, lesquels étaient coûteux à l’époque.

On leur a dit : « Voici la taille du marché » et AT&T a répondu : « Il n’y a pas lieu d’investir; nous ne pouvons pas composer avec un marché d’aussi petite taille. » Douze ans plus tard, AT&T a dépensé 12 milliards de dollars pour acheter McCaw Cellular et entrer sur le marché du téléphone cellulaire.

Les limites de notre imagination signifient que parfois on tarde trop à voir les possibilités. Cela explique en partie pourquoi nous avons eu la révolution technologique dans les années 1990. Personne ne voulait être laissé pour compte après avoir vu ce qui s’était passé avec la révolution de l’ordinateur personnel. Mais pourquoi Hewlett-Packard n’a-t-il pas investi dans le projet de Steve Wozniak? Ils ont jeté un coup d’œil aux micro-ordinateurs sur lesquels il travaillait et ont dit : « Il s’agit de jouets. Ils ne pourront pas satisfaire nos clients. »

Ils avaient raison. Il s’agissait de jouets. Ils ne pouvaient pas répondre aux exigences de leurs clients de longue date. Mais ils n’avaient pas compris qu’il s’agissait de technologies perturbatrices. Elles ont fini par être améliorées si rapidement qu’elles ont pris le dessus sur les technologies existantes.

Voilà donc la question qu’il faut se poser : à quelle vitesse pouvons-nous améliorer ces technologies? Voilà ce qui les rendra perturbatrices. Tout indique que les capteurs, les logiciels et la technologie des communications ont atteint un seuil de viabilité jamais atteint auparavant. C’est une option qui vaut certainement la peine d’être examinée.

[Français]

Le sénateur Boisvenu : Ma prochaine question a trait au volet social de la situation. Au cours des 20 dernières années, on a constaté l’arrivée et l’établissement massif des technologies dans les processus de production. Ceci a fait en sorte que beaucoup de

ranks of the structurally unemployed. For lack of education and training, they have been unable to adapt to the technological industrial development which evolved at such a phenomenal rate.

Automated vehicles will overtake manually driven ones, that is undeniable; might that not mean that people who do not have the capacity to understand the vehicle's operating system and technological programming will be left behind? Until fairly recently, you put your key in the ignition and started driving. Nowadays, the owner's manual is very thick and one must spend several evenings studying it to understand how the car works. Will this phenomenon not leave out a certain category of citizens, whether because of their age or their education? Is that a risk?

[English]

Mr. Michelson: It's interesting, because there are many stages or levels of vehicle automation. The level you're describing is the absolute top level, where everything is totally automated. But there are many other levels in between. Probably the biggest thing that vehicle automation will do is make vehicles safer. So even though the driver will still have an awful lot of control over the vehicle, they won't be responsible for the instantaneous decisions required to ensure that the driving is safe.

During the next 15 to 20 years, my prediction is that the biggest impact automated vehicles will have is on road safety. It means that the many people who are killed in road accidents each year will not be killed, because the software on board the vehicle will be able to avoid accident situations in a way that a human driver cannot because of their ability to react in split seconds and make good decisions. I would say that the lowest levels of vehicle automation are the ones that initially will be the most important, and they will have a direct impact on people's lives.

There are certain applications where total automation is required, perhaps where people are in unfamiliar places. It could be in situations like airports or in industrial settings where we'll probably see more of the higher levels of automation. I think the higher levels of automation will intrude very slowly into this space. But the safety aspects are the ones that I think are most important and the ones I'm looking forward to the most.

Senator Galvez: Mr. Michelson, I'm so sorry I couldn't make it for the beginning of your testimony, but I'm very interested in this topic and I hope you can answer my question.

As I understand it, as we go towards the electrification of transport, it seems electric cars are much simpler and have a smaller number of parts. I heard that a mechanical car has 2,000 parts

travailleurs se sont retrouvés sur le banc des chômeurs structurels. À cause d'un manque d'éducation et de formation, ils n'ont pas pu s'adapter au développement technologique industriel qui a évolué à une vitesse phénoménale.

Le véhicule automatisé va surpasser la notion manuelle, ce fait est indéniable; cela ne risque-t-il pas de mettre de côté des gens qui n'auront pas la capacité de comprendre le fonctionnement du véhicule et sa programmation technologique? Il n'y a pas si longtemps, on insérait la clé dans l'allumage et on prenait la route. Maintenant, le guide du conducteur est très épais et on doit consacrer plusieurs soirées à l'étudier pour comprendre le fonctionnement de sa voiture. Ce phénomène ne va-t-il pas écarter une certaine catégorie de citoyens, soit à cause de leur âge ou de leur éducation? Y a-t-il un risque?

[Traduction]

M. Michelson : C'est intéressant, car il y a différents degrés d'automatisation d'un véhicule. Celui que vous décrivez est le degré supérieur absolu, où tout est totalement automatisé. Mais il y a plusieurs autres degrés entre les deux. Il est probable que le principal changement qu'apportera l'automatisation des véhicules est de faire en sorte que la conduite automobile soit plus sûre. Cela signifie que, même si le conducteur demeure le maître de son véhicule, il ne sera pas responsable de prendre des décisions instantanées pour s'assurer que sa conduite automobile est sûre.

Je prédis que, au cours des 15 à 20 prochaines années, la principale répercussion de l'automatisation des véhicules sera la sécurité routière. Cela signifie que les nombreuses personnes qui seraient habituellement tuées chaque année dans un accident de la route ne mourront pas, car le logiciel à bord du véhicule sera capable d'éviter les accidents qu'un conducteur humain ne peut éviter en raison de la capacité du logiciel de réagir presque instantanément et de prendre une bonne décision. Je dirais que les degrés les plus faibles d'automatisation des véhicules seront ceux qui, au départ, seront les plus importants, car ils auront des retombées directes sur la vie des gens.

Il y a certaines applications où l'automatisation totale est nécessaire, peut-être lorsque les gens circulent dans des endroits qui ne leur sont pas familiers. C'est peut-être dans des aéroports ou dans des zones industrielles que nous verrons les plus hauts degrés d'automatisation. Je pense que les degrés supérieurs d'automatisation seront adoptés très lentement à cet endroit. Toutefois, je crois que les aspects de sécurité sont ceux qui sont les plus importants et ceux que j'ai le plus hâte de voir s'appliquer.

La sénatrice Galvez : Monsieur Michelson, je suis désolée d'avoir raté le début de votre témoignage. Cependant, le sujet de cette étude m'intéresse grandement et j'espère que vous pourrez répondre à ma question.

Si j'ai bien compris, en fait d'électrification des transports, il semble que les voitures électriques soient beaucoup plus simples et aient un nombre plus limité de pièces. J'ai entendu dire qu'une

compared with an electric car that will have only 200 parts. The mechanics are much simpler in electric cars. I just want you to confirm if this is true or not.

You are talking about intelligent transportation systems. We've been hearing that electrification and automation of cars will solve, as my colleague said, the congestion and the environmental pollution. I believe that to get to that point, the key thing is the communication: vehicle-to-vehicle and vehicle-to-infrastructure. If that works, by trial and error, as you just mentioned, we will get to this intelligent, smart and efficient transport.

My second question is this: To have this efficient communication, will it be controlled centrally, like for airports and planes? There is one central station that controls everything. Or do you imagine that several stations will control the traffic and the circulation of the multiple users of the road? As you said, there will be a transition, but there are also cyclists and pedestrians. There is common transport and tracks. How do you see the future? How are we going to get to this efficient point?

Mr. Michelson: That's a very good question.

Ultimately, I think it's going to be a distributed system. It will start, for example, with something like where there's an accident on a street that's blocking traffic, a sensor will detect that there has been an accident and the traffic is blocked, and it can send a message to all vehicles. It wouldn't be that much more complicated than the Garmin and Tom Tom devices that many people currently use.

Many of these channels already exist through various wireless systems that are often transmitted as FM sub-carriers. They can say that there's an accident here, and the device can make a decision to take a detour. If they transmit back what they're doing, then the central system can send messages out saying other vehicles are going over here and let people know where the congestion is. I think a distributed system is likely what will happen.

To me, as an engineer, the frustrating part is we're almost there in so many ways. We're so near the tipping point, but we're not quite there yet. I think when it all of a sudden happens, when it reaches a certain critical mass, I think it will be exciting. But we're closer than you might think.

Senator Galvez: Who will be in control of this? Tom Tom?

Mr. Michelson: That's one of the questions right now. Most of the traffic congestion information is provided by cell carriers like TELUS and Rogers. That is provided to places like Google, Nokia and various other companies that then supply this data

voiture mécanique compte 2 000 pièces, alors qu'une voiture électrique n'en comptera que 200. La mécanique est beaucoup plus simple dans la voiture électrique. Pouvez-vous me dire si c'est vrai?

Vous avez parlé de systèmes de transport intelligent. Comme mon collègue l'a indiqué, nous avons entendu dire que l'électrification et l'automatisation des voitures vont régler les problèmes de congestion et de pollution environnementale. D'après moi, pour arriver à ce point, il faudra surtout compter sur la communication : de véhicule à véhicule et de véhicule à infrastructure. Si cela fonctionne, comme vous venez de le mentionner, nous arriverons par tâtonnement à nous doter d'un système de transport intelligent, fûté et efficace.

J'ai une deuxième question pour vous. La communication efficace devra-t-elle être contrôlée par une centrale, comme dans les aéroports? Dans un aéroport, c'est la tour centrale qui contrôle tout. Ou imaginez-vous qu'il y aura peut-être aussi plusieurs centrales qui contrôleront la circulation des nombreux usagers de la route? Comme vous l'avez dit, il devra y avoir une transition, mais il y aura également des cyclistes et des piétons. Sans compter les pistes et les voies de transport communes. Comment envisagez-vous l'avenir? Comment allons-nous en arriver à ce stade d'efficacité?

M. Michelson : C'est une très bonne question.

En fin de compte, je crois qu'on aura affaire à un système en réseau. Prenez par exemple un accident qui bloque la circulation dans une rue. Un capteur détectera ensuite l'accident et la congestion conséquente et pourra envoyer un message à tous les véhicules. Le système ne sera pas bien plus compliqué que les technologies de Garmin et de Tom Tom qui sont déjà employées dans des appareils couramment utilisés par les gens.

Bon nombre de ces canaux existent déjà grâce à différents systèmes sans fil qui sont souvent transmis grâce à des intermédiaires FM. Lorsque l'appareil apprend qu'un accident a eu lieu, il peut décider de faire un détour. S'il y a une retransmission de cette manœuvre, le système central peut alors envoyer des messages aux autres véhicules pour indiquer ce qui se passe à cet endroit et signaler le lieu de congestion. Je présume que nous verrons probablement un système en réseau.

Pour un ingénieur comme moi, ce qu'il y a de frustrant, c'est que, à bien des égards, nous sommes si près du but. Nous sommes très près du point de bascule, mais nous n'y sommes pas encore. Je crois qu'à un certain moment, nous atteindrons une masse critique qui permettra d'en arriver à cette phase, et ce sera emballant. Nous sommes toutefois plus près que vous ne l'imaginez.

La sénatrice Galvez : Qui contrôlera ce système? Tom Tom?

M. Michelson : C'est une des questions que nous nous posons en ce moment. La majeure partie des renseignements sur la congestion automobile est fournie par des fournisseurs de services cellulaires comme TELUS et Rogers. Ces données sont transmises

through to Tom Tom. There are many players involved, but a lot of this stuff happens as commercial transactions. It isn't as visible and open as some of the more open protocols.

Some of this already exists, but it's all done as proprietary solutions that are supplied to individual companies. If these were things were more open, many of us think that would be nice. Of course, the companies themselves like the current situation.

[Translation]

Senator Saint-Germain: Good evening.

I am interested in the public infrastructure that will be required for us to fully benefit from autonomous vehicles. I am talking about completely automated vehicles, which should arrive on the market around 2030. Do you believe that in Canada, all the necessary infrastructure — whether telecommunications or roadway infrastructure — will be ready in time so that the full capacity of autonomous vehicles is not delayed? That is the first part of my question.

Secondly, with respect to funding this public infrastructure, have you already thought of the financial arrangements that will be necessary to develop and fund this necessary public infrastructure?

[English]

Mr. Michelson: I think we'll probably find that the infrastructure and funding will happen in layers and stages. I don't think automated vehicles initially will be used everywhere. We may, for example, have dedicated lanes on freeways that are used by automated vehicles, at which point you can then operate in fully automated mode; and then, when you go off the freeway, you will have to go back to a role in which the driver has more control.

This will happen in stages and layers, because we're not going to turn our infrastructure inside out, every square kilometre of our city completely set up for automated vehicles. It will happen in stages. We have to be very selective about which areas we're going to make automated- ready, and then which layers we will gradually add on.

History has shown us that most technology advances in stages and layers. It's very difficult to make an abrupt transition. I think we'll see that, instead of having HOV lanes on freeways, we'll have automated vehicle lanes. Then we'll gradually see more and more stretches where, if congestion is a particular issue, this is where automated vehicles will be allowed to go to full level 5, for example. It will happen in stages, step by step.

à des entreprises comme Google, Nokia et diverses autres sociétés qui relaient ensuite ces renseignements à Tom Tom. De nombreux acteurs ont un rôle à jouer, mais une bonne partie de tout cela se déroule sous forme de transactions commerciales qui ne sont pas aussi visibles ni ouvertes que le sont certains protocoles.

Ce type de communication existe déjà, mais il est réalisé par l'intermédiaire de solutions brevetées qui sont fournies à des entreprises individuelles. Nous sommes nombreux à souhaiter que ces transactions soient plus ouvertes. Évidemment, pour leur part, les entreprises préfèrent la situation actuelle.

[Français]

La sénatrice Saint-Germain : Bonsoir.

De mon côté, je m'intéresse aux infrastructures publiques qui seront nécessaires pour qu'on ait la capacité de tirer pleinement profit des avantages d'une voiture autonome. Je parle du véhicule complètement autonome, qui arriverait sur le marché vers les années 2030. Croyez-vous que, au Canada, l'ensemble des infrastructures nécessaires — qu'il s'agisse des télécommunications ou des infrastructures routières — seront prêtes à temps pour ne pas retarder la pleine capacité d'utiliser les véhicules autonomes? C'était le premier volet de ma question.

Deuxièmement, en ce qui concerne le financement de ces infrastructures publiques, avez-vous déjà réfléchi à un montage financier, qui devrait être associé au développement et au financement des infrastructures publiques nécessaires?

[Traduction]

M. Michelson : Je crois que l'on s'apercevra probablement du fait que l'infrastructure et le financement seront gérés par étape. Je ne crois pas que, au départ, les véhicules automatisés seront utilisés partout. Il se pourrait, par exemple, qu'il y ait des voies réservées aux véhicules automatisés sur les autoroutes; à ce stade, il sera possible de s'en remettre pleinement à l'automatisation. Ensuite, une fois que le véhicule aura quitté l'autoroute, il faudra que le conducteur exerce un contrôle accru sur la conduite.

Cela se produira en étapes, car nous n'allons pas chambouler notre infrastructure, chaque kilomètre carré de notre ville, pour l'adapter complètement aux véhicules automatisés. Cela se produira par étapes. Nous devons être très judicieux quant aux secteurs que nous adapterons aux véhicules automatisés et dans quel ordre nous procéderons.

L'histoire nous a démontré que la plupart des progrès technologiques se sont faits par étapes. Il est très difficile de procéder à une transition abrupte. Je crois que nos voies pour le covoiturage sur les autoroutes seront remplacées par des voies réservées aux véhicules automatisés. Graduellement, nous ajouterons des segments où, si la congestion est particulièrement épineuse, les véhicules automatisés seront autorisés à passer au niveau 5, par exemple. Cela se produira par étapes.

[Translation]

Senator Saint-Germain: When it comes to funding public infrastructure, do you think there are possibilities for partnerships, among others, with users who would be user-payers, with industry and with public transit? Should government alone be responsible for infrastructure-related costs, for upgrading and developing infrastructure, especially telecommunications infrastructure? You can give us your personal opinion, if you have not studied that specific aspect.

[English]

Mr. Michelson: It's something that often comes up, the cost of the infrastructure and how this will be paid for. Of course, some people advocate public-private partnerships, which then imply there will be tolls charged, so there will be a return on investment. This can be very challenging in some ways. People do not like paying tolls, so this will be a real impediment to adoption.

In British Columbia we just had a provincial election where one of the key platforms was considering bridge tolls, and the results of the election proved what the electorate thought. The current party in power has acknowledged that this was probably not the best platform to run on.

Yes, it's tempting to talk about using tolls and partnerships of this sort. Ultimately, I think our challenge as engineers, and what I always tell people, is to make these systems scalable and relatively inexpensive. We have to acknowledge the fact that we're going to have to deploy a lot of devices. If cost were no object, our job would be over tomorrow, but cost is an object. Therefore, the challenge is up to us in the technical community to make the infrastructure inexpensive so that it doesn't become an overwhelming problem. That's our challenge and one that I hope our community is willing to accept.

If we go in layers and stages, I don't think replacing HOV lanes with automated vehicle lanes on freeways will incur a lot of cost. The way to do it is to always take the path of least cost, or at least try to reduce our costs. Then I think we'll probably find that it will happen seamlessly. That's my personal opinion.

Senator Saint-Germain: I hope that if we have tolls, we'll have access to electronic payment.

Mr. Michelson: Absolutely.

Senator Saint-Germain: It would be great.

Mr. Michelson: It's noteworthy that all this current connected vehicle technology has actually evolved from the original electronic toll collection concept, the 5.9 gigahertz band that is used for DSRC, which was originally allocated for electronic toll

[Français]

La sénatrice Saint-Germain : En ce qui a trait au financement des infrastructures publiques, croyez-vous qu'il y a des possibilités de partenariat, entre autres, avec les utilisateurs qui seraient des utilisateurs-payeurs, avec l'industrie et les transporteurs publics? Est-ce que le gouvernement devrait assumer seul les coûts liés à l'infrastructure, à la mise à niveau et au développement des infrastructures, en particulier les infrastructures de télécommunication? Vous pouvez nous donner votre opinion personnelle, si vous n'avez pas étudié cet aspect spécifiquement.

[Traduction]

M. Michelson : C'est un sujet qui revient régulièrement sur le tapis, c'est-à-dire le coût de l'infrastructure et qui paiera. Bien entendu, certaines personnes préconisent des partenariats public-privé, ce qui sous-entend qu'il y aura des postes de péage afin d'obtenir un rendement sur l'investissement. Cela peut être très difficile à certains points de vue. Les gens n'aiment pas les péages, si bien qu'il sera très difficile de les convaincre de l'adopter.

En Colombie-Britannique, nous venons d'avoir des élections provinciales dans lesquelles un des principaux partis envisageait des ponts à péage. Les résultats de ces élections ont révélé ce que les électeurs en pensaient. Le parti actuellement au pouvoir a reconnu que ce n'était probablement pas là une des meilleures idées sur lesquelles fonder un programme électoral.

Je l'admets, il est tentant de parler de péage et de partenariats de ce genre. Toutefois, au bout du compte, je crois que notre défi en tant qu'ingénieurs, et c'est ce que je dis toujours aux gens, est de faire en sorte que ces systèmes soient adaptables et relativement peu coûteux. Nous devons reconnaître le fait que nous devons faire preuve d'ingéniosité. Si le coût n'était pas important, notre travail serait terminé demain, mais le coût est important. Par conséquent, il nous incombe en tant que spécialiste technique de faire en sorte que l'infrastructure soit peu coûteuse afin qu'elle ne devienne pas un problème insurmontable. C'est notre défi, et j'espère que notre communauté est prête à le relever.

Si nous y allons étape par étape, je ne crois pas que remplacer les voies réservées au covoiturage par des voies réservées aux véhicules automatisés sur les autoroutes coûtera très cher. La meilleure façon d'y parvenir est toujours de prendre la solution qui coûte le moins cher, ou du moins d'essayer de réduire nos coûts. Je pense qu'alors nous trouverons que cela se produira sans anicroche. C'est mon opinion personnelle.

Le sénateur Saint-Germain : J'espère que, si nous avons des postes de péage, nous aurons accès au paiement électronique.

M. Michelson : Absolument.

Le sénateur Saint-Germain : Ce serait fantastique.

M. Michelson : Fait à noter, toute la technologie actuelle pour les véhicules automatisés découle en vérité du concept de télépéage initial, la bande de 5,9 gigahertz qui était utilisée pour la CDCD, qui était au départ destinée au télépéage. En Europe et

collection. In Europe and Asia, it was used exclusively for that. It was only in North America that it became a full connected vehicle band. ETC is still the basis for all of these technologies that are used.

Senator Bovey: When you talked about tolls being electronic, of course the congestion charge zones in London are all electronic, just by scanning licence plates.

We talked a bit about urban and rural. Of course, Canada has other challenges, too, and they are called the climate and the environment. I wonder what you see as some of the challenges in making all this technology available for minus 40 to plus whatever, and ice and snow. What do you see in terms of your challenges ahead as you plan for environmental conditions? You talked about it rolling out in layers and stages. Will those layers and stages be geographical?

Mr. Michelson: Yes. Probably our largest centres that have urban traffic congestion problems are the ones that will be used first. I think we'll find a lot of this is going to be used in industrial settings far before they're used in civil settings. We're already seeing in the mining industry, for example, that a lot of proprietary automated vehicle solutions are being used, simply because they can afford it and because the safety issues are serious enough that it makes sense to use it.

Senator Bovey: Is it working in northern British Columbia?

Mr. Michelson: And in northern Alberta, a place like Syncrude, where they've been experimenting with automated vehicle technology for use in the open-pit mines there. It seems to be working pretty well. They seem to be happy with it.

These are being used in limited areas, under controlled conditions. People think it's wonderful that Google went out and started to put all this automated vehicle technology on open roadways and such, but I think the reality is that the widespread deployment will happen in industrial settings first, and then they will gradually find their way into civil settings.

Senator Eggleton: Picking up on that and on your opening comments, I didn't realize there were 620,000 kilometres of resource roads in British Columbia. Is that not an opportunity to be able to demonstrate these vehicles? Building public confidence is important as well. Before many people will get into a vehicle, either a level 4 or certainly a level 5, there has to be some confidence that this can manoeuvre within urban traffic and all the challenges that are faced there. Isn't this resource road possibility a good opportunity to demonstrate the technology, particularly under rough terrain and rough weather conditions?

en Asie, elle était utilisée exclusivement pour cela. Ce n'est qu'en Amérique du Nord qu'elle est devenue une bande pour les véhicules automatisés. Le télépéage demeure encore le point de départ de toutes ces technologies qui sont utilisées.

La sénatrice Bovey : Vous avez parlé du télépéage. Dans les zones congestionnées de Londres visées par un péage, tous les paiements se font de manière électronique, simplement en balayant les plaques d'immatriculation.

Nous avons parlé un peu des secteurs urbains et ruraux. Bien entendu, le Canada a d'autres défis, soit le climat et l'environnement. Quels sont selon vous les défis à relever pour que cette technologie fonctionne dans un climat où il peut faire moins 40 degrés Celsius, avec de la glace et de la neige? Quels seront les défis à relever sur le plan des conditions environnementales? Vous avez dit que la mise en œuvre se fera par étapes. Ces étapes seront-elles déterminées par la géographie?

M. Michelson : Oui. Il est probable que nos grands centres qui souffrent d'un problème de congestion routière en profiteront les premiers. Je pense que nous découvrirons que cette technologie sera utilisée dans des milieux industriels bien avant d'être appliquée dans des milieux urbains. Par exemple, le secteur minier fait déjà appel très souvent à des véhicules automatisés brevetés simplement parce qu'il peut se le permettre et parce que les questions de sécurité sont suffisamment importantes pour en justifier l'utilisation.

La sénatrice Bovey : Est-ce que cela fonctionne dans le Nord de la Colombie-Britannique?

M. Michelson : Et dans le Nord de l'Alberta, une entreprise comme Syncrude, où ils expérimentent depuis quelque temps les technologies de véhicules automatisés dans les mines à ciel ouvert. Les résultats semblent très concluants. Ils semblent en être très heureux.

Ces véhicules sont utilisés dans des secteurs restreints, dans un contexte très contrôlé. Les gens trouvent fantastique que Google ait entrepris déjà de faire rouler leur véhicule automatisé sur les routes, et cetera, mais je pense que la réalité, c'est que le déploiement à grande échelle de cette technologie se fera dans des milieux industriels tout d'abord, et ensuite elle fera graduellement son entrée dans la société civile.

Le sénateur Eggleton : À ce propos, je reviens sur vos observations préliminaires. Je ne savais pas qu'il y avait 620 000 kilomètres de routes d'accès aux ressources en Colombie-Britannique. N'est-ce pas là une belle occasion de faire la démonstration de ces véhicules? Il importe, aussi, de gagner la confiance du public. Avant que bien du monde veuille embarquer dans un véhicule, que ce soit au niveau 4, ou certainement au niveau 5, il faut que les gens aient confiance que ledit véhicule sache manoeuvrer dans la circulation urbaine et composer avec tous les défis qu'il présente. Est-ce que ces routes d'accès aux ressources ne présenteraient pas une bonne occasion de faire la démonstration de la technologie, particulièrement en terrain accidenté et dans des conditions météorologiques difficiles?

Mr. Michelson: I totally agree with that. It's a tremendous opportunity.

Regarding resource roads, they rely exclusively on VHF voice radios. In B.C., for example, the ministry of forests has worked with the spectrum management people from ISED to come up with a fairly complicated scheme of radio channels and various procedures. But they would really like to look into doing something that places less of a requirement on the operator, so there is the idea of using automated vehicle technologies and advanced connected vehicle technologies to reduce some of these risks.

Unfortunately, these resource roads in some cases are one and a half lanes wide. They have to know where everybody is going, and making good decisions is important. I've talked to people who have had close calls, and they say, "We really wish we had a more automated system to make sure we don't run into that situation."

I totally agree; it's a tremendous opportunity for Canada, from coast to coast. B.C. has more resource roads than we do regular urban roads. But even in Quebec and Ontario, there are a lot of resource roads. Yes, it's a tremendous opportunity.

Senator Eggleton: Following up on that, is the forestry industry getting involved in trying to develop those possibilities?

Mr. Michelson: FPIInnovations is the forestry industry's national research and development arm, and they are in the early stages of pushing this through. Of course, if there was interest and support from the government, this would make their job much easier. They're certainly interested in pursuing this.

The Chair: Colleagues, before we go in camera, I'd like to thank Mr. Michelson for his presentation.

I'd also like to pay homage to our colleague Senator Runciman, who is participating in his last Transport and Communications meeting. As you know, we will not be meeting next week, and by the time we come back in September, Senator Runciman, after 35-odd years in politics, will have retired to do something else.

I've been working with Senator Runciman for nine years. We didn't always agree, obviously. That's not that obvious, but trust me, it happened a few times. I want to pay homage. Thirty-five years of dedication to the Canadian public and to the people of Ontario is something that deserves to be recognized. I'm sure it will be recognized elsewhere, but as chairman of this committee, I am taking the privilege of being probably the first one.

Hon. Senators: Hear, hear!

M. Michelson : Je suis tout à fait d'accord. C'est une superbe occasion.

Au sujet des routes d'accès aux ressources, les communications s'y font exclusivement par radio VHF. En Colombie-Britannique, par exemple, le ministère des Forêts a travaillé avec le groupe de gestion du spectre du ministère de l'Innovation, des Sciences et du Développement économique à l'élaboration d'un système plutôt complexe de chaînes radio et de procédures diverses. Ils aimeraient néanmoins pouvoir envisager quelque chose qui soit moins exigeant pour l'opérateur, et c'est pourquoi il y a cette idée d'utiliser les technologies avancées de véhicules automatisés et de véhicules connectés pour réduire en partie ces risques.

Malheureusement, ces routes d'accès aux ressources ne font parfois qu'une voie et demie de large. Il leur faut connaître l'itinéraire de tout le monde, et il importe de prendre les bonnes décisions. J'ai parlé à des gens qui avaient frôlé la catastrophe, et ils disent : « Nous aimerions vraiment avoir un système plus automatisé pour nous assurer de ne pas nous retrouver dans ce genre de situation. »

Je suis tout à fait d'accord; c'est une superbe occasion pour le Canada, d'un bout à l'autre du pays. La Colombie-Britannique a plus de routes d'accès aux ressources que de voies urbaines ordinaires. Mais même le Québec et l'Ontario ont de nombreuses routes d'accès aux ressources. Oui, c'est une superbe occasion.

Le sénateur Eggleton : Dans le même ordre d'idées, est-ce que le secteur forestier fait quelque chose pour exploiter ces possibilités?

M. Michelson : FPIInnovations, l'organe national de recherche et de développement du secteur forestier, vient d'entamer une démarche en ce sens. Évidemment, si le gouvernement manifestait de l'intérêt et offrait un soutien, cela leur faciliterait beaucoup la tâche. Il est clair que c'est quelque chose qui les intéresse beaucoup.

Le président : Chers collègues, avant de poursuivre à huis clos, je tiens à remercier M. Michelson pour son exposé.

Je tiens aussi à rendre hommage à notre collègue, le sénateur Runciman, qui assiste aujourd'hui à sa dernière réunion du Comité des transports et des communications. Comme vous le savez, il n'y aura pas de réunion la semaine prochaine, et à notre retour en septembre, le sénateur Runciman aura pris sa retraite après quelque 35 années en politique pour faire autre chose.

Je travaille avec le sénateur Runciman depuis neuf ans. Nous n'avons pas toujours été d'accord, bien évidemment. Cela ne semble pas si évident, mais croyez-moi, c'est arrivé à quelques reprises. Je tiens à lui rendre hommage. Trente-cinq ans de dévouement au public du Canada et à la population de l'Ontario méritent d'être soulignés. Je ne doute pas que ce sera souligné dans d'autres contextes, mais en ma qualité de président du comité, j'ai le privilège d'être probablement le premier à le faire.

Des voix : Bravo!

Senator Runciman: I want to briefly return the compliments. I sat in on this committee on a number of occasions when you were the chair and was impressed with the way you handled this committee and the chairmanship and the guidance you provide. I asked to be on this committee specifically because of how impressed I was with you, Mr. Chair.

The Chair: You're very kind.

(The committee continued in camera.)

Le sénateur Runciman : J'aimerais brièvement rendre la pareille. J'ai siégé à quelques reprises à ce comité alors que vous le présidiez. J'ai été impressionné par votre manière de diriger les travaux et par les orientations que vous avez fournies. J'ai demandé à siéger à ce comité précisément parce que vous m'avez impressionné, monsieur le président.

Le président : Vous êtes bien aimable.

(La séance se poursuit à huis clos.)

WITNESSES

Tuesday, June 13, 2017

Carillon Information Security Inc.:

Patrick Patterson, President.

CoinDesk:

Nolan Bauerle, Director of Research.

Ford Motor Company of Canada, Limited:

Blake Smith, Director, Sustainability, Environment and Safety Engineering.

Wednesday, June 14, 2017

As an individual:

David Michelson, Co-Chair of the Intelligent Transportation Systems Society of Canada and Professor, University of British Columbia.

TÉMOINS

Le mardi 13 juin 2017

Carillon Information Security Inc. :

Patrick Patterson, président.

CoinDesk :

Nolan Bauerle, directeur de recherche.

Ford du Canada limitée :

Blake Smith, directeur en chef, Durabilité, environnement et ingénierie de la sécurité.

Le mercredi 14 juin 2017

À titre personnel :

David Michelson, coprésident, Société des systèmes de transport intelligents du Canada, et professeur, Université de la Colombie-Britannique.