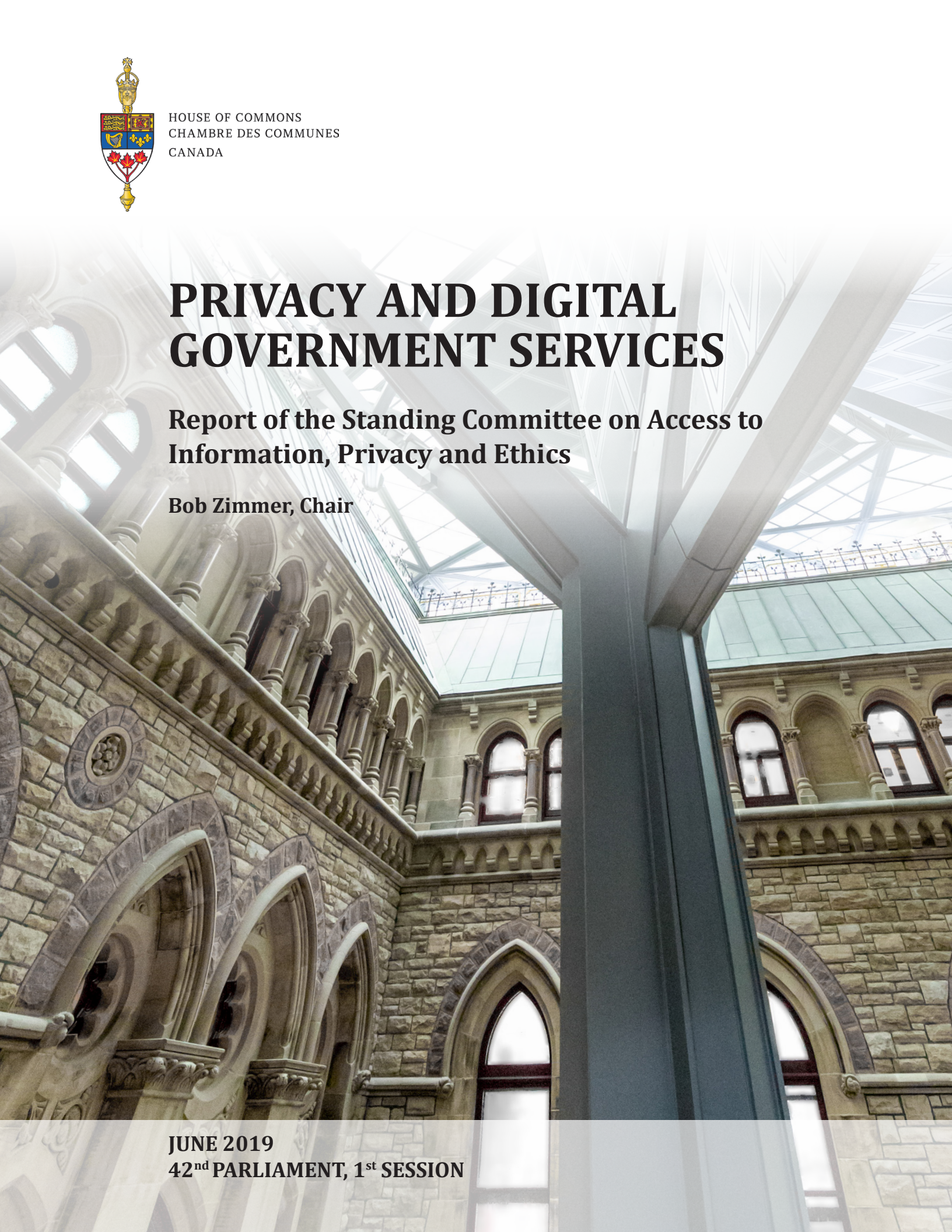

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

PRIVACY AND DIGITAL GOVERNMENT SERVICES

Report of the Standing Committee on Access to Information, Privacy and Ethics

Bob Zimmer, Chair

JUNE 2019
42nd PARLIAMENT, 1st SESSION

PRIVACY AND DIGITAL GOVERNMENT SERVICES

Report of the Standing Committee on Access to Information, Privacy and Ethics

Bob Zimmer
Chair

JUNE 2019

42nd PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committee presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Bob Zimmer

VICE-CHAIRS

Charlie Angus
Nathaniel Erskine-Smith

MEMBERS

Frank Baylis
Mona Fortier
Jacques Gourde
Hon. Peter Kent
Michel Picard
Raj Saini
Anita Vandenbeld

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Ziad Aboultaif
René Arseneault
Nathan Cullen
Fayçal El-Khoury
Andy Fillmore
David de Burgh Graham
Cheryl Hardcastle
Gord Johns
Michael Levitt
Brian Masse
Irene Mathyssen
Robert J. Morrissey
Hon. Joyce Murray

Eva Nassif
Anne Minh-Thu Quach
Churence Rogers
Francis Scarpaleggia
Gagan Sikand
Adam Vaughan

CLERKS OF THE COMMITTEE

Michael MacPherson
Jean-Denis Kusion

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Alexandra Savoie, Analyst
Maxime-Olivier Thibodeau, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

NINETEENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*)(vii) and the motion adopted by the Committee on Tuesday, February 6, 2018, the Committee has studied the privacy of digital government services and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1 on the modernization of Canada's privacy laws:

That the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* be modernized by adopting the Committee's recommendations regarding these acts in the following reports:

- **Report 4—Protecting the Privacy of Canadians: Review of the Privacy Act (December 2016)**
- **Report 12—Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act (February 2018)**
- **Report 16—Addressing Digital Privacy Vulnerabilities and Potential Threats to the Canadian Democratic Electoral Process (June 2018)**
- **Report 17—Democracy at Risk: Risks and Solutions in the Age of Disinformation and Data Monopoly (December 2018) 19**

Recommendation 2 on data minimization:

That the Government of Canada commit to uphold data minimization, de-identification of all personal information at source when collected for research or similar purpose and clarify the rules of consent regarding the exchange of personal information between government department and agencies. 19

Recommendation 3 on public trust in government:

That the Government of Canada work to inform Canadians about the coming shift to digital government and involve them in the design and development of infrastructure needed to deliver digital government services. 25

PRIVACY AND DIGITAL GOVERNMENT SERVICES

INTRODUCTION

On 6 February 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) adopted a motion that the Committee undertake a study on digital government services to understand how the government can improve services to Canadians while protecting their privacy and security.[1]

The Committee held 12 meetings with witnesses on the subject between 22 March 2018 and 9 April 2019, during which it heard a total of 33 witnesses. It also received four written submissions.

This report summarizes the testimony heard by the Committee and makes eight recommendations.

THE ESTONIAN MODEL

The Committee's study was inspired by the model of digital government in Estonia, which is one of the most advanced countries in terms of digital government services. To better understand this model and how it has been possible to create a digital society in Estonia, the Committee received, as the first witnesses to this study, representatives of the Estonian Academy of e-Governance.

A. Representatives from Estonia

Regarding the founding principles of Estonia's e-governance model, Liia Hänni, a senior expert on e-democracy with Estonia's e-Governance Academy, said that it is based on the conviction that an e-governance structure and model should be a platform for all society.[2] She said that the Estonian model has three important components:

- the Estonian government gives a strong digital identity to Estonians;

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI], *Minutes of Proceedings*, 42nd Parliament, 6 February 2018.

2 ETHI, *Evidence*, 1st Session, 42nd Parliament, 22 March 2018; e-Governance Academy of Estonia, *About Us*.

- there are extensive data and digital resources (there are hundreds of databases to store digital data); and

- interoperability between the numerous datasets is realized by the X-Road platform, which connects all datasets into one uniform system.[3]

Ms. Hänni said that the Estonian experience is that private data is better protected in the digital environment than in a paper environment. Estonians can track digital information exchanges that occur, who accessed their file and why. It is often impossible to know who has accessed paper documents and why.[4]

She also said that digital signatures are commonplace in her country. Estonians no longer need to sign paper documents, and digital signatures bring the country "a huge economy of resources, time, and money."[5]

Regarding cybersecurity in the Estonian model, Raul Rikk, national cybersecurity program director with Estonia's e-Governance Academy, said that every Estonian has an ID card with a chip that contains a cryptoprocessor. When citizens use them, they actually use an encryption system.[6] ID cards are issued by the government, and the government process of identifying persons and issuing ID cards ensures that in Estonia, nobody can steal someone else's identity.[7]

Mr. Rikk said that data collection by various Estonian authorities is based on the "once only" principle:

> We have not centralized the databases, but the logic behind no overlapping databases is that we don't collect the same data in different databases. For example, if we have a population registry containing basic information about citizens and residents, then when police forces create their own police database, we don't allow them to collect the same basic information there. They have to take the most recent information from the population registry. The idea is that different state institutions have authority over certain data. If they are allowed to collect this data and keep it in their database, then

3 ETHI (2018), 0905 (Liia Hänni, Senior Expert, e-Governance Academy of Estonia).

4 Ibid., 0940.

5 Ibid., 1010.

6 Ibid., 0915 (Raul Rikk, Director, National Cyber Security Program, e-Governance Academy of Estonia).

7 Ibid., 0930.

> nobody else can collect and keep the same data. In this way, we keep the data in order at the state level.[8]

Mr. Rikk specified that no single agency in Estonia is able to get access to all exchanged information at once. Only authorized individuals can access datasets. Access permissions vary for citizens, government officials and the police.[9] There is also a record of when citizen data is accessed, that citizens can consult on the government portal in order to see who saw what information and when. Only concerned citizens can see all the information collected about themselves.[10]

Mr. Rikk also said that since information is decentralized, the potential vulnerabilities in an information management system can be managed. Estonia does not have a single huge database containing all the information about its citizens. Therefore, if a person hacks into and damages certain systems, the damage will be limited to a single separate system containing information and not to the entire system.[11] Mr. Rikk described how information is exchanged between databases in Estonia:

> Some of them are in the public sector and some of them are in the private sector. We make the connectivity between the databases through the secure data exchange environment. We call it the X-Road. It's a state-controlled environment. Everybody who wants to be connected to this data exchange environment has to, first of all, implement certain security regulations, security guidances, be up to the standards, etc. They have to apply to be part of this secure data exchange environment. It means that we keep an eye on the data exchange. We control that. We don't go into the data itself, but we control how the data exchange happens. Everything is encrypted, as I mentioned, logged, and time-stamped. The way we get information from the databases is not by going directly into the database. Instead we get the information through the electronic services … There is e-police, e-school, e-tech support. This is like a presentation format. The electronic service takes predefined data from different databases and then presents it.[12]

Mr. Rikk stressed the importance of maintaining data integrity and confidentiality while providing data access, by protecting it and preventing it from being changed by anyone other than the relevant individual.[13]

---

8 Ibid., 0915.

9 Ibid., 0925.

10 Ibid., 0930.

11 Ibid., 0950.

12 Ibid.

13 Ibid., 0920.

Lastly, regarding private-sector access to data on citizens, Mr. Rikk said the following:

> Each time the private sector wants to use personal data or they want to get connectivity to the X-Road environment, they have to prove their need to the data protection inspectorate. They have to justify why they need it. The data protection inspectorate allows them to use the personal data … The private sector generates certain information, and they can provide it to the government through the secure X-Road.[14]

B. Comments of other witnesses on the Estonian model

Ann Cavoukian, former Ontario privacy commissioner and expert in residence at the Privacy by Design Centre of Excellence at Ryerson University, said that the Estonian model was an excellent model of decentralization and that a decentralized model has several pots of information, each one a database with information that can be accessed for a particular purpose.[15] In her view, "the more you have decentralized pots of information the greater the likelihood the data will remain and will be retained for the purposes intended and not used across the board for a variety of purposes that were never contemplated."[16]

The Privacy Commissioner of Canada, Daniel Therrien, said the following:

> While the Estonian model is often discussed for its technological architecture, I was struck by the fact that officials emphasized the greater importance, in their view, of attitudinal factors, including the need to overcome silos in state administration leading to reuse of personal information for purposes other than those for which it was collected.
>
> This could be seen as validation of the view that our *Privacy Act* needs to be re-examined and that—quote, unquote—"legal barriers" should be eliminated. I would note, however, that in Estonia the elimination of silos did not lead to a borderless, horizontal management of personal data across government. Rather, in the Estonian model, reuse, or what we would call sharing of information, appears to be based on legislation that sets conditions generally consistent with internationally recognized fair information practice principles and with the GDPR [the European Union's *General Data Protection Regulation*].
>
> …

14 Ibid., 1020.

15 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1555 (Ann Cavoukian, Privacy by Design Centre of Excellence, Ryerson University).

16 Ibid.

> As to the technological aspects of the Estonian model, our understanding is that there is an absence of a centralized database. Rather, access is granted through the ability to link individual servers through encrypted pathways with access or reuse permitted for specific lawful purposes. This purpose-specific access by government agencies likely reduces the risk of profiling.
>
> We understand that further privacy and security safeguards are attained through encryption and the use of blockchain. This is in line with one of our recommendations for revisions of the *Privacy Act* in 2016, namely, to create a legal obligation for government institutions to safeguard personal information.[17]

Mr. Therrien did raise a few questions about the Estonian model. First, noting that no system is entirely secure, he believes it would be important to know what mitigation measures are in place in Estonia in the event of a security breach. Second, he questioned how the value proposition of a model such as Estonia's, which lies in the analysis of data held by the government as a whole, could be reproduced in Canada, given the decentralized datasets and the legislative regime limiting data reuse in Canada.[18]

Cybersecurity expert Chris Vickery raised doubts about the Estonian representatives' claims that there have never been any privacy breaches or issues. He said he is certain that the Estonian system is not impenetrable.[19]

David Eaves, a lecturer in public policy with the digital project HKS at Harvard Kennedy School, highlighted three parts of the Estonian model he considers important:

1. there is a database for each piece of information collected about an Estonian citizen (e.g., one for addresses, one for drivers' licences, etc.);

2. the information is linked together by a unique identifying ID to make it easy to pull together disparate information about a citizen in order to get a very clear view about the person and provide this information to the various government agencies as they are trying to deliver services; and

3. these databases are accessible to all government officials across all government agencies.[20]

---

17 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1540 (Daniel Therrien, Privacy Commissioner of Canada).

18 Ibid.

19 ETHI, *Evidence*, 1st Session, 42nd Parliament, 5 February 2019, 1615 and 1655 (Chris Vickery).

20 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1550 (David Eaves, Lecturer in Public Policy, Digital HKS, Harvard Kennedy School).

Mr. Eaves also submitted a brief to the Committee in the form of a paper he co-authored entitled "Lessons from Estonia on digital government."[21] In the paper, the authors write that, unlike a number of countries that take a siloed approach to digital government services, some countries, such as Estonia, use a standardized system that allows government departments and agencies to share sign-in information and databases that support online services. These systems can talk to each other, which means that new services can be developed and offered quickly and cheaply. In a siloed approach, since departments digitize their services and work independently, they duplicate effort to collect all the personal information required, which is inefficient and expensive. Duplication sometimes even occurs within the same department.

In a "platform government," standards are defined so that the core sets of public tools and databases—the platforms—can be reused by the public and private sector to drive down costs and simplify services. Government platforms are seen as core public infrastructure and a source of competitive advantage. However, the authors acknowledge that the shift to a platform approach to government poses a number of challenges, including:

- whoever controls the servers will control the government. It may therefore be in the government's interest to deny access to certain parts of the systems (e.g., to private companies participating in the infrastructure) and control how they are developed;

- private software vendors will determine the architecture of services and offerings and could design them in such a way as to impede competition; and

- it could be difficult to convince public servants and the public to trust common platforms in a system built around siloed departments.

Alex Benay, Chief Information Officer of the Government of Canada, said that although Canada is different from Estonia both culturally and legally speaking, his organization has learned a lot from the Estonian example, including how to share data in a secure way and how to deliver digital services and increase privacy at the same time.[22]

---

21 David Eaves and Ben McGuire, "Lessons from Estonia on digital government," Policy Options, 7 February 2019. The article contains, among other things, a figure illustrating the X-Road secure data exchange environment that allows for secure data exchange in Estonia (see Figure 4).

22 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1555 (Alex Benay, Chief Information Officer of the Government of Canada).

Mr. Benay believes there is a lot that Canada can learn from what the Estonians have done with their X-Road data sharing platform and he told the Committee that Estonian officials were invited twice to Canada to help the government of Canada in creating a similar platform in accordance with Canada's laws, regulations and other contingencies. According to Mr. Benay, "the beauty with this system, if it proceeds down this road, is that we will be able to bake in accessibility, privacy and security. We'll also be able to determine how we move data around in the Government of Canada, based on a core set of principles."[23]

Matthew Anthony, Vice-President, Incident Response and Threat Analysis with the Herjavec Group, a cybersecurity firm, cautioned the Committee against holding up Estonia as a standard for our transformations in Canada, since it had certain advantages that Canada does not.[24]

Finally, Marina Mandal, Vice-President, Banking Transformation and Strategy with the Canadian Bankers Association (CBA), said that the CBA's white paper cites two countries: Estonia and India. With respect to Estonia, she said that "the similarities between the lessons learned from Estonia for Canada is the paramount importance of privacy and data security." She also said that the similarities with Estonia stop there.[25]

PART I—FIRST STEP TOWARDS DIGITILIZATION OF GOVERNMENT SERVICES: ADOPTING AN APPROPRIATE LEGISLATIVE FRAMEWORK

Several of the witnesses heard by the Committee mentioned that for a shift to digital government services at the level of the Government of Canada to be successful, it is first necessary to ensure that an appropriate legislative framework is in place.

A. Modernization of privacy laws

Ms. Cavoukian said that Canadian privacy laws are "so dated" and an update is needed.[26]

---

23 Ibid., 1615.

24 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 February 2019, 1535 (Matthew Anthony, Vice-President, Incident Response and Threat Analysis, Herjavec Group).

25 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2019, 1545 (Marina Mandal, Vice-President, Banking Transformation and Strategy, Canadian Bankers Association).

26 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1635 (Ann Cavoukian).

> I totally support Commissioner Daniel Therrien's call to the federal government to upgrade the PIPEDA [*Personal Information Protection and Electronic Documents Act*], for example, which dates from the early 2000s. He also said we need to add privacy by design to the new law because, after all, they have embedded it in the GDPR. We need new tools. We need to be proactive. We need to identify the risks and address them up front.
>
> …
>
> Upgrading the laws is absolutely essential. Giving the commissioner the much-needed authority that he needs but now lacks is essential. I can say, having been a privacy commissioner for three terms, that I had order-making power. I rarely used it, but that was the stick that enabled me to engage in informal resolution with organizations, government departments that were in breach of the privacy law. It was a much better way to work.
>
> I had the stick. If I had to issue an order, I could do that. That's what Commissioner Therrien lacks.[27]

Michael Geist, Canada Research Chair in Internet and e-Commerce Law with the Faculty of Law at the University of Ottawa, appeared at the same time as Ms. Cavoukian. He believes that digital government services will engage a far more complex ecosystem that involves not just the questions of the suitability, in the digital age, of the *Privacy Act*, which applies to the collection and use of personal information by federal government institutions.[28] Rather, given the overlap between public and private, between the various orders of government, and between domestic and foreign, he said that the Canadian government should conduct a more holistic assessment that recognizes that the delivery of digital government services will involve more than just one law or set of regulations.[29] Mr. Geist nevertheless identified three shortcomings with the *Privacy Act* which he believes merit correction:

1. The *Privacy Act* desperately needs a mandate for public education and research similar to what the Commissioner has done about raising awareness about PIPEDA.[30]

27 Ibid.

28 Ibid., 1545 (Michael Geist, Canada Research Chair in Internet and e-Commerce Law, Faculty of Law, University of Ottawa).

29 Ibid. For example, these changes could affect the *Privacy Act*, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), trade agreements that feature data localization and data transfer rules, open government policies, and private sector standards and emerging technologies.

30 Ibid.

2. The *Privacy Act* falls woefully short of meeting the standards of a modern privacy act. The government should be subject to limits similar to those applicable to the private sector for collecting only that information that is strictly necessary for its programs and activities.[31]

3. The *Privacy Act* should require greater transparency and impose on government, as is now the case with the private sector under PIPEDA, data breach disclosure rules and the obligation to issue transparency reports.[32]

For his part, Mr. Therrien said that a potential barrier to information sharing between government departments lies in sections 4 to 8 of the *Privacy Act* and that these rules should be re-examined with an eye to improve government services in the digital age. He added that any new legislation designed to facilitate digital government services must respect privacy as a human right. He reiterated the Office of the Privacy Commissioner's (OPC) recommendations from 2016 on modernizing the *Privacy Act* and added one recommendation: that the public sector adopt the concept of privacy by design.[33] He repeated that it is essential to look very closely at the legal framework within which either data will be shared from one department to another, or a second department will be able to reuse data that the first department has. Technologically speaking, he said that data banks should not be able to talk to each other unless there is a legal authority to do that.[34]

Mr. Therrien also mentioned that the OPC should have powers similar to those of the Estonian data protection authority, which has an explicit proactive role, can issue binding orders, can commence criminal proceedings and can impose fines where data is processed in an unlawful manner.[35]

Lastly, Mr. Therrien said that if laws are amended to facilitate the introduction of digital government services, the OPC should be consulted. The OPC is prepared to play a proactive role with respect to digital government services, give advice as early as

31 Ibid., 1550.

32 Ibid.

33 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1535 (Daniel Therrien).

34 Ibid., 1600.

35 Ibid., 1540.

possible and play an oversight role once systems are adopted. However, it must have the legal powers needed to play that role.[36]

Mr. Eaves pointed out that in Estonia, before any technical work began on their systems, the Estonians did a lot of work to update their privacy laws for the 21st century and to create systems of logs and audits so that citizens could see who was accessing their data, pose questions about whether that access was legitimate, and challenge authorities accordingly.[37]

Mr. Benay also said that a newly created body, the Enterprise Architecture Review Board, applies a privacy lens to all major government projects. He also said that his organization has discussions with the Office of the Privacy Commissioner about potential legislative impediments and believes that this dialogue will continue to increase as digital services expand.[38]

Mr. Benay said that his organization works closely with the Department of Justice and with Innovation, Science and Economic Development Canada to meet the requirement imposed on the Treasury Board Secretariat (the Enterprise Architecture Review Board) to catalogue the potentially required legislative amendments.[39] Mr. Benay said that his organization set aside two years to review certain legislation that might hinder information sharing.[40] He pointed out that as part of this review process, the organization he leads must also review several data-sharing agreements between existing departments.[41]

For Aaron Snow, Chief Executive Officer of the Canadian Digital Service, legislation is often the slowest and most encumbered of all routes to the solutions, and it can result in unintended consequences. He argued that instead, efforts should focus on the smallest and fastest unit of governance when possible to avoid going into the process of

36 Ibid., 1610.

37 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1555 (David Eaves).

38 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1615 (Alex Benay).

39 Ibid., 1640.

40 Ibid. On 12 April 2019, the Treasury Board of Canada Secretariat (TBS) provided the Committee with the document "Service Strategy—Legislative Inventory," which provides a preliminary review of the legislative provisions governing how departments may share information, including with other departments, provinces and third parties. At the same time, the Committee received written responses from TBS to supplement the responses provided orally by officials on 19 February 2019.

41 *Ibid*., 1650.

creating and amending laws.[42] Mr. Snow said that the Canadian Digital Service is a new digital consultancy in Treasury Board. Its mandate is to provide hands-on help to federal departments to make digital services faster, simpler, more accessible and secure, as well as to help build capacity in those departments and provide modern service design and delivery.[43]

B. Privacy by design, data minimization and consent

In addition to the modernization of privacy legislation, several witnesses discussed important privacy concepts, including design privacy, data minimization and consent. Some also shared their vision of the ideal model of digital government.

1. Privacy by design

Ms. Cavoukian said that privacy by design is a positive sum model that achieves two positive gains: privacy and security, and technological innovation.[44] This privacy by design framework is predicated on proactively embedding all the needed privacy protective measures into the design of operations and policies for all services and in terms of data utility.[45] She said that this principle, contrary to adopting or amending legislation, which could be slow, needs to be used as a proactive means of preventing the harms from arising.[46]

Ms. Cavoukian said that privacy by design must also be incorporated into the development of technologies used by the federal government. For instance, with respect to blockchain, she said that this technology does not guarantee anonymity, that it could have negative sides and that it has already been hacked in the past. For it to be effective, it must be introduced by incorporating privacy into the technology from the start.[47]

42 Ibid., 1640 (Aaron Snow, Chief Executive Officer, Canadian Digital Service).

43 Ibid., 1540.

44 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1540 (Ann Cavoukian).

45 Ibid.

46 Ibid., 1600.

47 Ibid., 1615.

Mr. Therrien said that privacy by design should be applied on the ground by the bureaucracy and by departments in the delivery of services.[48] He also discussed the importance of this concept when it comes to artificial intelligence:

> [P]rivacy by design ensures that AI is implemented in such a way that the information that feeds the system, first, has been lawfully obtained, second, is reliable, and third, does not discriminate on the basis of prohibited grounds of discrimination, but is based on objective factors of analysis.[49]

Mr. Therrien also illustrated how this principle is applied by discussing the right to privacy as a human right:

> When I say that privacy is a fundamental right, it is a concept that should be recognized, not only in the law, but also by government bodies that, day after day, implement technological and other systems to collect data and to administer public programs, including by technology … If we have a choice between providing a service in a way that endangers privacy and providing the same service differently, but just as effectively, in a way that protects privacy, the concept of protecting privacy from the design stage tells us that we should choose the latter option.[50]

2. Data minimization, de-identification and consent

Ms. Cavoukian said that data minimization is a key concept in the privacy world that also results in multiple positive gains at the same time.[51]

With regard to data de-identification, Ms. Cavoukian used her experience as a consultant for Sidewalk Labs (SWL) to provide a concrete example of the importance of this concept. She said that she was approached to help SWL incorporate privacy by design in the future smart city that could emerge in Toronto. From the outset, she insisted that data collected in this future smart city be de-identified at source. Later on, SWL revealed that it would create a "civic data trust" that could consist of SWL, the various orders of government involved and various intellectual property companies. SWL then said that it was unable to guarantee de-identification. Following this announcement, Ms. Cavoukian left her position as a consultant. She now works with Waterfront Toronto

48 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1620 (Daniel Therrien).

49 Ibid., 1640.

50 Ibid., 1630.

51 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1540 (Ann Cavoukian).

to move things forward. She believes that as soon as decisions are left to companies, it is certain that the data collected will not be de-identified at source.[52]

As for the amounts of data collected by the government, Ms. Cavoukian said that having more data is far from preferable. The government should only use data collected for that particular purpose, unless it has obtained additional consent. Even when the government has good intentions (e.g., to use personal information to inform people about funds they could receive), it is important to not deviate from the standard. It is entirely possible that citizens do not want their government to use data collected for a specific purpose to raise awareness.[53] She said that privacy is all about the control that people have over the use of this data. As soon as the government starts stretching that out because it believes that the government knows better, she believes that this could take the government down the path of inappropriate surveillance.[54]

Ms. Cavoukian said that people do not provide the government with their personal information so it can use it however it wants; they provide it for a particular purpose (e.g., paying their taxes) and the government cannot do whatever it wants with this personal information.[55] This is called purpose specification and use limitation, which she believes is fundamental to privacy.[56]

Regarding consent to the collection and use of personal information and data overuse, Mr. Geist said that "our standards of consent have become so polluted by the low standards found in PIPEDA, which I think have been widely abused, that few people actually trust what consent means at this stage." He recommended finding mechanisms to ensure that meaningful consent is truly meaningful, informed consent.[57] As for the problem of data overuse, he said the following:

> I think at the end of the day you need to ensure you have governments, just like companies, that recognize that where they become overly aggressive with using data, because they feel they can, they cause enormous harm to that information ecosystem,

52 Ibid., 1610.

53 Ibid., 1625.

54 Ibid.

55 Ibid., 1645.

56 Ibid.

57 Ibid., 1640 (Michael Geist).

> and ultimately undermine public confidence not only in them but also, I think, in governments more broadly.[58]

Mr. Therrien also noted that it was important that the government only collect the information it really needs, even if the information could be considered to be in the public domain.

> We have to be careful in calling this information public. As you have just said, it is still possible to identify the person associated with a car, their behaviour, and so on. So, even if the information is called public, we have to wonder whether the information is actually personal, and what authority a given department has to collect it. It varies from department to department. Even though the information is in the public domain, collecting it has to be linked to a mandate of the department in question. That is a very important condition in the current legislation. It could be made stronger, along the lines of some recommendations we made in connection with amending the *Privacy Act*.[59]

Mr. Vickery said that minimizing the amount of personal information a government collects is also beneficial from a cybersecurity perspective.[60] Jason Kint, Chief Executive Officer of Digital Content Next, suggested that when someone is online, their expectations should be the same as when they are buying something at the store, meaning that they should not be asked information that is not necessary.[61]

Amanda Clarke, Assistant Professor of the School of Public Policy & Administration of Carleton University, noted that there needs to be a realistic approach concerning citizens' capacity to give informed consent, noting that it has been demonstrated that it would take approximately 76 working days for the average person to read all of the digital privacy policies they agree to in a year.[62] She also discussed data governance issues from a consent perspective, saying that we need to ask questions about how data can be combined, whether citizens feel comfortable with the state contacting them directly, and how they want government departments to be able to access their data.[63]

---

58 Ibid., 1650.

59 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1550 (Daniel Therrien).

60 ETHI, *Evidence*, 1st Session, 42nd Parliament, 5 February 2019, 1655 (Chris Vickery).

61 Ibid., 1700 (Jason Kint, Chief Executive Officer, Digital Content Next).

62 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1540 (Amanda Clarke).

63 Ibid., 1640.

3. Ideal model for digital government

Mr. Benay believes that the ideal digital government model would provide digital services to Canadians on the IT platform of their choice or in person at a Service Canada office. The system would be developed with the help of Canadians and would have privacy and data protection requirements and access to information standards built in by design. Mr. Benay would also like to create a system that supports interoperability across different orders of government.[64]

Mr. Snow believes that the ideal model for digital government would:

- be fully transparent and able to explain how the service is being delivered, what the steps are and how it all works, and
- be flexible and adaptable.[65]

Mr. Snow said that the Canadian Digital Service tries to demonstrate the five following principles in all its projects:

1. applying research and design practices that put people first, not rules and processes, by focusing on the people who use government services;
2. delivering and improving continuously by keeping systems patched and up to date;
3. assuming that failures will happen and planning accordingly because "[c]ybersecurity best practice is to make the rational assumption that failures and breaches will happen, and to plan accordingly;"
4. working transparently: in full view of the team and, whenever possible, the public; and
5. creating strong feedback loops between delivery and policy by working with and listening to users, putting working prototypes in front of them as quickly as possible and continuously improving services to learn which

64 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1620 (Alex Benay).

65 Ibid. (Aaron Snow).

policies are working, how others are not, and how they should be updated.[66]

Mr. Anthony believes that government services must be digitized slowly, awaiting the necessary technology, such as artificial intelligence and automation controls, for greater support throughout this transformation.[67] He listed the following important steps from the Data Strategy Roadmap for the Federal Public Service:

- develop a strategy;
- provide clarity on data stewardship;
- develop standards and guidelines for governance;
- improve recruitment to gather the skills needed; and
- develop technology systems that support the strategy.[68]

4. Ethics of algorithms and artificial intelligence

On the topic of the Digital 9 partners' work (or D9, which includes, in addition to Canada, Estonia, Israel, South Korea, New Zealand, the United Kingdom, Uruguay, Mexico and Portugal), Mr. Benay said that Canada had led a joint declaration on the use of artificial intelligence.[69] He believes that Canada's artificial intelligence initiatives and the tools it is developing (such as the vendor catalogue and the "algorithmic impact assessment" tool set, which has been jointly implemented around the world) have made it a true leader in the field.[70]

As for the ethics of algorithms and artificial intelligence, Mr. Benay said that countries will automate their services according to their values framework. In Canada, the directives implemented by Mr. Benay's agency ensure that black boxes are not making decisions on behalf of human beings, for example.[71] In terms of algorithmic transparency, Mr. Benay said that the governance of algorithms is uncharted territory

66 Ibid., 1540 and 1545.

67 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 February 2019, 1535 (Matthew Anthony).

68 Ibid.

69 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1555 (Alex Benay).

70 Ibid., 1625 and 1700.

71 Ibid., 1700.

and that some mechanisms, such as the architecture review board, exist to ensure that algorithms reflect Canadian values and that these values will be respected throughout the process—from procurement to deployment.[72]

In light of the above, for any shift toward Government of Canada digital government services to be successful, the Committee makes the following recommendations:

Recommendation 1 on the modernization of Canada's privacy laws:

That the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* be modernized by adopting the Committee's recommendations regarding these acts in the following reports:

- **Report 4—Protecting the Privacy of Canadians: Review of the Privacy Act (December 2016)**
- **Report 12—Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act (February 2018)**
- **Report 16—Addressing Digital Privacy Vulnerabilities and Potential Threats to the Canadian Democratic Electoral Process (June 2018)**
- **Report 17—Democracy at Risk: Risks and Solutions in the Age of Disinformation and Data Monopoly (December 2018)**

Recommendation 2 on data minimization:

That the Government of Canada commit to uphold data minimization, de-identification of all personal information at source when collected for research or similar purpose and clarify the rules of consent regarding the exchange of personal information between government department and agencies.

72 Ibid., 1705.

PART II—MEASURES TO ENSURE THE SUCCESS OF A SHIFT TOWARDS DIGITAL GOVERNMENT SERVICES

A. Building public confidence in digital government services

Jerry Fishenden, a visiting professor at the Surrey Business School working at the Centre for the Digital Economy of that school in the United Kingdom since 2014, said that it is important to ensure that citizens are the custodians of their personal information and have the access and control that are necessary to decide what they want to share with different officials.[73]

Ms. Cavoukian noted two examples that have eroded public confidence in the government, in her view: the failure to subject political parties to privacy laws and the Prime Minister of Canada's support for Statistics Canada's efforts to obtain highly sensitive financial information from the public.[74] Mr. Geist agreed with Ms. Cavoukian.[75]

Mr. Geist added that improving applicable federal privacy rules would foster public confidence in government services by ensuring, for example, that there are adequate safeguards and transparency and reporting mechanisms to give the public the information it needs about the status of their data and appropriate levels of access.[76]

Mr. Therrien said that since Canadians are concerned these days that their privacy is not being respected, an incremental implementation—where the government has a chance to demonstrate that the system deserves trust—may reassure the population.[77]

Ms. Clarke also recognized that there needs to be trust in the system for it to work. She suggested that a model that focuses on accountability for learning could generate a government culture that respects privacy but also allows companies to be more innovative in their services.[78]

She mentioned the need for more surveys and studies that ask people whether they would agree to have their data used for purposes other than that for which it was

---

73 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 March 2018, 0915 (Jerry Fishenden, Visiting Professor, Centre for the Digital Economy, Surrey Business School, University of Surrey, United Kingdom).

74 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1655 (Ann Cavoukian).

75 Ibid. (Michael Geist)

76 Ibid., 1550.

77 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1600 (Daniel Therrien).

78 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1650 (Amanda Clarke).

collected by presenting a value proposition. She said that there needs to be a value proposition put forward other than asking citizens if they want to be surveilled and have their data abused. Clearly the answer to the question about surveillance will be negative, even though that is not what is meant when talking about digital government services.[79] Mr. Roy agreed, suggesting that a broader public debate on the level of comfort of citizens with data sharing should be held.[80]

Ms. Clarke also said that, while some Canadians may not be asking the government to proceed with digital government services, they could be open to these transformations if they are shown how easy it could become to apply for a service and see their information already populated, or how the organization of services around life events could make their interactions with the state much more seamless.[81]

Mr. Eaves said that in Canada, people are comfortable giving information to the federal government because they do not necessarily believe that the government has the competency to weave information together to create a story about them.[82] There is a kind of social contract between the government and Canadians that there will be limited use of their personal information. Therefore, he believes that there needs to be a very intentional dialogue about what the new social contract between the government and the public might look like in a digital government. For example, in Estonia, one important piece of that social contract is that the individual who provides information to the government can, in exchange, see who has accessed their information, why it was accessed and where access appears to have been inappropriate, file a complaint.[83]

Mr. Eaves also argued that the voluntary participation of the public is necessary for the shift towards digital government services to succeed.[84] Mr. Eaves added that the digital shift should not end up creating a two-track system where the wealthy, who do not often interact with the government, contribute very little information and the government knows less about them, while those most in need, who are marginalized

79 Ibid., 1700.

80 Ibid., 1605 and 1615 (Jeffrey Roy, Professor, School of Public Administration, Dalhousie University).

81 Ibid., 1640.

82 Ibid., 1555 (David Eaves).

83 Ibid., 1620.

84 Ibid., 1630 and 1655.

and less able to protect themselves, have to provide the government with a lot of information.[85]

With respect to the idea that improving government services and privacy are not at odds with each other, Mr. Benay argued that, thanks to technological improvements that allow these protections to be built in from the concept and development stages, these two ideas do not conflict.[86]

His organization has taken steps to promote digital services and better protect Canadians' personal information, such as

- a set of digital standards that help government departments and agencies design better services for Canadians; and

- rules and guidelines based on best practices to help departments and agencies with the digital transition.

According to Mr. Benay, these measures support open standards and open source programs, "cloud first" principles, as well as ethical data collection and data security principles. The changes will help staff work more efficiently government-wide thanks to a better convergence of technology and policies and opportunities for dialogue from the beginning of the procurement process.[87]

He believes that these measures are key in order for the Government of Canada to develop a comprehensive digital strategy for the long term, with the priority being the integration of security and privacy at the investment and design stage of government services, programs and operations.[88]

Mr. Benay said that his organization was also active in the following areas:

- a public sector digital academy created in partnership with the Canada School of Public Service;

- rules to commonly accept and trust digital identities, in cooperation with provincial and territorial governments, as well as the private sector;

85 Ibid.

86 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1530 (Alex Benay).

87 Ibid., 1535.

88 Ibid.

- a digital identity ecosystem to support their use to access services across jurisdictions;
- an initiative called “Sign In Canada” to allow users across the country to access government services online using their federated trusted digital identity;
- a digital exchange platform to help enable departments to share their data with each other and the outside world (similar to the X-Road platform used in Estonia);
- a new Enterprise Architecture Review Board made up of business and technology representatives from across government (on security, privacy and data, applications, service delivery, moving to the cloud, artificial intelligence and governance challenges, for example89);
- the possibility of providing a “tell us once” user experience: his organization “is currently examining government business processes, policies and legislation to identify any barriers to implementing this service vision”;
- close cooperation with the OPC to benefit from advice on plans and initiatives to advance digital government;
- the creation of the first list of AI suppliers that had to demonstrate that they have the necessary resources and skills and have adopted ethical AI practices, in cooperation with Public Services and Procurement Canada; and
- a new recruitment model (the “Government of Canada talent cloud”), an experiment to facilitate the hiring process and adapt to the market.[90]

According to Mr. Benay,

> our service strategy must adhere to a fundamental principle: no one should fall through the cracks. Trust will likely play a role as well. We’ll have to show people that we can meet our commitments and that they can have confidence in the system—hence the

89 Ibid., 1555.

90 Ibid., 1550.

> importance of being transparent about the services we will provide and the policies we develop.[91]

As for the importance of educating the public about digitizing services, Mr. Benay said that the scale of public education initiatives is growing in certain countries and that the educational aspect should be included in government programmes as society progresses towards digital technology.[92] He gave the example of Uruguay, where iPads have literally been brought into people's homes to educate them, show them how to interact with the government and explain what to do and what not to do—if their mobile device is hacked, for instance.[93]

Della Shea, Vice-President of Privacy & Data Governance and Chief Privacy Officer with Symcor, presented three core tenets that she believes underpin public trust in the management of personal information:

1. privacy by design and data stewardship;
2. the role of trusted service providers in a digital ecosystem; and
3. a consistent legislative framework.[94]

With respect to privacy by design, Ms. Shea recommended establishing controls on the way governments design their systems. She added that data stewardship and being an effective data steward is about actually operationalizing the accountability model that has been set forth under Canadian privacy legislation.[95]

As for the role of trusted service providers in a digital ecosystem, she argued that it is critical for government to establish a working model that consists of trusted service providers and intermediaries in the digital ecosystem whereby organizations would be held to a consistent standard "to minimize the likelihood of systemic vulnerabilities, but more generally to provide confidence in the digital ecosystem and digital service delivery."[96]

---

91 Ibid., 1625.

92 Ibid., 1655.

93 Ibid.

94 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2019, 1535 (Della Shea, Vice-President, Privacy & Data Governance and Chief Privacy Officer, Symcor).

95 Ibid.

96 Ibid.

Regarding the third tenet, Ms. Shea stressed the importance for all players in the digital landscape, both private sector and public sector, to follow consistent and robust privacy legislation.[97]

Finally, regarding seniors' participation in the digital society in Estonia, Ms. Hänni said that the Estonian government introduced several special programs to encourage them in that direction when it decided to transition to digital.[98]

In light of the above information, the Committee recommends that:

Recommendation 3 on public trust in government:

That the Government of Canada work to inform Canadians about the coming shift to digital government and involve them in the design and development of infrastructure needed to deliver digital government services.

B. Change of culture in the public service

Ms. Hänni said that electronic government development is not so much about technology but rather about innovation and innovative co-operation among different government departments. She said that having a good system of digital government means making radical changes to public servants' attitudes, overcoming silos in government, and getting all organizations to work together.[99]

Mr. Therrien said that before systems are implemented more broadly, senior government officials should have an attitude of ensuring that safeguards are in place before the systems are implemented in order to avoid cases such as Phoenix, where senior officials deliberately decided not to put in place strong monitoring of who had access to personal information in the system because it would have been costly and resulted in delays.[100]

As for Ms. Clarke, she highlighted the possible tensions between digital government and government tradition. While it is often said that federal public servants do not have an appropriately robust appreciation for privacy, Ms. Clarke instead hears an alternative narrative in her research: that some public servants are overly zealous, an attitude that

97 Ibid.

98 ETHI, *Evidence*, 1st Session, 42nd Parliament, 22 March 2018, 1000 (Liia Hänni).

99 Ibid., 1010.

100 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1555 (Daniel Therrien).

can really undercut scope for innovation and improvements to government services, as well as undermine the efficiency and effectiveness of the daily operations of government.[101]

Ms. Clarke also pointed out that the kind of crosscutting policy analysis that draws on data from multiple departments is increasingly important, but that under the current legislation, vertical accountability regimes, and corporate information management strategies favour the siloing of data in the public service. She recommended a more balanced approach to privacy and security to avoid costs to the efficiency and effectiveness that can come from overly prioritizing these issues.[102]

She also said that the Westminster system of parliament is behind some of the tensions around vertical accountability structures and the horizontal government platform model that is being increasingly supported. She believes that there are ways to overcome these challenges. There should be a focus on models of horizontal accountability or shared accountability if digital government services are to be rolled out on a larger scale.[103] Mr. Eaves agreed with that proposition.[104]

Mr. Eaves added that the technical challenges of building digital government services infrastructure are going to be significantly smaller than the governance challenges. He suggested that finding the critical service that would have the highest impact on Canadians and the one that would be most helpful to make easy could help collect the necessary data from the various orders of government in a practical and real project.[105]

According to Mr. Snow, culture change is a slow process that does not usually happen effectively with a single directive that everybody should just start behaving and thinking differently all at once. Rather, its success is measured by observing whether the methods, practices or tools put in place to carry out one project are used to carry out another project.[106]

101 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1530 (Amanda Clarke).

102 Ibid.

103 Ibid., 1640.

104 Ibid., 1615 (David Eaves).

105 Ibid., 1605.

106 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1630 (Aaron Snow).

Ms. Shea said that the data strategy road map for the federal public service published last fall "outlines a comprehensive vision to overcome silos and leverage data as a valuable asset" and encouraged the government to

> design a maturity model that will scale to the future, one that not only considers privacy and security at the foundational level of digitizing government services but also contemplates a fully digitized society where everyone and everything is connected to a fluid and ever-expanding ecosystem.[107]

In light of the above information, the Committee recommends that:

Recommendation 4 on the change of culture in the public service:

That the Government of Canada work to ensure collaboration and information sharing between departments and government agencies with respect to the implementation of digital government services in order to ensure effective deployment of these services on a large scale.

Recommendation 5 on the secure exchange of data:

That the Government of Canada promote the connection of various departmental databases to a digital backbone to allow for secure and controlled sharing of data.

C. Guaranteeing Internet access

Mr. Geist suggested that one important factor related to introducing digital service standards is to ensure that everyone can access the network so they can obtain the digital services created.[108] He believes that in order for the government to roll out a growing number of digital services, it needs to make concrete investments to guarantee universal, affordable Internet service for everyone. Until this point is reached, he believes that there needs to be parallel service sets to ensure that everyone has access to services.[109]

The Committee agrees with Mr. Geist and recommends:

107 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2019, 1540 (Della Shea).

108 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1620 (Michael Geist).

109 Ibid., 1625.

Recommendation 6 on guaranteeing Internet access:

That the Government of Canada work to ensure that reliable, affordable Internet access is extended to rural and remote areas even as services are digitized in areas already serviced.

D. Governance of Indigenous Peoples' data and the impact on digital government services

The issue of Indigenous data sovereignty was raised by Ms. Clarke. According to her,

> There are very unique concerns at play here concerning the way the Government of Canada collects and uses data relating to indigenous people, and in particular the way services are delivered to those communities. Given ongoing ways in which that data has been used to marginalize and oppress indigenous peoples, I think it's really incumbent upon this committee to particularly carve out some space for that issue.[110]

The Committee agrees with Ms. Clarke and recommends:

Recommendation 7 on the governance of Indigenous people's data:

That the Government of Canada consult with Indigenous peoples when developing digital government services.

PART III—OTHER CONSIDERATIONS

A. Digital identity

The identity card program failed in the United Kingdom, according to Mr. Fishenden, partly because the Home Office was seen as the arbiter of the new national identity register and the fact that people were going to have to store all their biometrics and personal data with one single government department.[111] In his opinion, there should be more effective ways of linking proven identities to the different data silos or lockers so that, for example, individuals could prove who they were to the National Health Service

110 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1540 (Amanda Clarke).

111 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 March 2018, 0905 (Jerry Fishenden).

and confirm the link to their health records without potentially exposing it to other government departments without their consent.[112]

He stressed that, in the United Kingdom:

> [The program] made the fundamental error of assuming that having a single identity number for everything would be a good thing in a highly computerized age, whereas, [with] the Estonian model, which is based around a unique ID but keeps your data segmented, … citizens still feel that they're in control of their identity rather than the state being in control.[113]

In this regard, Andre Boysen, Chief Information Officer, SecureKey Technologies, said that Canada, the United States, the United Kingdom, Australia, New Zealand and many European countries are against the idea of a national ID card, especially due to the danger of having all the data in one place.[114]

About this risk, Mr. Boysen explained that a single identifier for government purposes should be avoided, because it would allow one individual to see everywhere another individual has gone across the Internet; it would create a genuine surveillance network. Instead, Mr. Boysen's company designed a system based on triple-blind privacy to solve this problem, requiring users to submit a plurality of identifiers.[115]

With regard to the use of the blockchain for this purpose, Mr. Boysen provided the following explanation:

> What we're using blockchain for is integrity proofs. We use it as a method to implement triple blinds so the issuer of the data can demonstrate that they wrote the data and that's the same data that they gave to the user to present. The receiver can get the data and know that it hasn't been altered. Then the consumer can have confidence that we're not oversharing data.[116]

Ms. Cavoukian, for her part, said that if digital identity is well protected and encrypted and that access to it is limited, it can actually improve access to services.[117]

---

112 Ibid.

113 Ibid., 0925.

114 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 February 2019, 1555 (Andre Boysen, Chief Information Officer, SecureKey Technologies Inc.).

115 Ibid., 1625.

116 Ibid., 1615.

117 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 January 2019, 1630 (Ann Cavoukian).

Ira Goldstein, Senior Vice-President, Corporate Development, Herjavec Group, said that digital identity is a key building block in the transformation of government services, but that the government should tread lightly when transforming its services to ensure that privacy and security are top priorities.[118] He mentioned Canada Revenue Agency's EFILE system as a successful case of digital transformation. He said that

> [d]igitizing government services will be welcomed by the public if managed and messaged thoughtfully. The upside of this effort is more access for historically marginalized groups and geography, so the opportunity cannot be ignored.[119]

For his part, Mr. Anthony recommended that the government start by

> looking at all of the different identifiers [it has] now and picking places where [it] could integrate and create a single authentication system that would allow high-fidelity identification for transactions that are happening within and around the government services.[120]

Rene McIver, Chief Security Officer, SecureKey Technologies, believes that ways must be found to combine the prime factors of identity so that people can confirm that their clients are who they say they are. She mentioned the need for trusted networks with citizen participants, whose control over their own data and privacy will underpin its security.[121]

Ms. McIver recommended using the "triple-blind" privacy approach, according to which:

> The receiving organization does not need to know the actual issuer of the information, only that it comes from a trusted source. The issuer does not need to know who the receiving organization is. And the network operators are not exposed to the unprotected personal information.[122]

With this approach, none of the participants in the transaction gets a complete picture of it. Ms. McIver added that this proven formula has been recognized by the privacy community, including by the Office of the Information and Privacy Commissioner of Ontario. According to Ms. McIver, the key factors for success in this matter are:

---

118 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 February 2019, 1530 (Ira Goldstein, Senior Vice-President, Corporate Development, Herjavec Group).

119 Ibid.

120 Ibid., 1625 (Matthew Anthony).

121 Ibid., 1540 (Rene McIver, Chief Security Officer, SecureKey Technologies Inc.).

122 Ibid.

- ensuring citizen acceptance and trust;
- having the potential to reach a large user base quickly;
- connecting the trusted parts of the digital economy such as finance, telecommunications, government and commerce; and
- ensuring public- and private-sector participation.[123]

According to Mr. Boysen, an identity has three components and they need to be kept separate:

1. the identity question: who are you?
2. authentication: are you the same person who showed up the first time?
3. authorization: what can I do inside your service?[124]

Ms. Mandal said that "we're still tethered to an analog model that relies on presenting physical documents to establish our identity in multiple daily transactions that we have with public services, businesses and each other."[125] She identified three major flaws with the current system:

1. it is outdated;
2. even today's technology-based approaches are clumsy: the two-factor identification sequence used online can be easily compromised, and users must remember dozens of log-in credentials; and
3. inefficient methods of establishing identity are a drag on economic growth.[126]

123 Ibid.

124 Ibid., 1625 (Andre Boysen).

125 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2019, 1530 (Marina Mandal, Vice-President, Banking Transformation and Strategy, Canadian Bankers Association).

126 Ibid.

Ms. Mandal believes that digital ID allows people to verify their identity electronically, using a combination of existing systems and newer biometric tools, such as fingerprints and facial recognition.[127]

Ms. Mandal said that updates made in 2018 to the *Bank Act* expressly allow banks to provide identification, verification and authentication services beyond the needs of their own operations. She also said that the CBA produced a white paper last year that "lays out a clear path for making digital ID a reality in Canada."[128] Ms. Mandal then said that the CBA took into account Canada's unique characteristics, advanced institutions and sophisticated infrastructure to develop a framework for what could work here.

Ms. Mandal called for a federated model of digital ID that would create linkages between federal and provincial identity management systems. She said that, for example, the federal government has social insurance and passport information, but the provinces manage health cards and driver's licences.[129]

Ms. Mandal believes that the Canadian banking sector is ideally situated to manage this federated digital ID system because of their existing interconnected electronic systems and the fact that banks are held to a high standard when it comes to collecting and safeguarding the personal information of their customers.[130] She said that the federated model involves passing legislation that would allow businesses and government to accept digital ID.[131]

Ms. Mandal also highlighted the important work done by the Digital Identification and Authentication Council of Canada in creating a pan-Canadian trust framework. The trust framework is expected to be completed in 2020, given that discussion drafts are being produced right now for public comment.[132]

127 Ibid.

128 Ibid.

129 Ibid.

130 Ibid.

131 Ibid., 1535.

132 Ibid., 1545.

B. Procurement of digital government services technology and governance of personal information

Ms. Clarke said that procurement is instrumental to digital service design and delivery. She suggested using a method called design thinking, which begins early on with extensive research into users and how they are going to use the service. Once the research is completed, all ensuing procurement and service design activities must be carried out based on its findings.[133]

She suggested that digital government services be organized around life events, adding that citizens do not care which government department does what and they do not want to have to go through a series of siloed websites. It is a matter of optimizing time and resource management—transacting with the government should not take too long. Ms. Clarke added that the implementation of any model of horizontal, platform government should begin with an appreciation of user needs.[134]

Ms. Clarke also said that the government is not directly involved in delivering many of its digital services. She added that certain questions arise when privately owned interfaces become the only or easiest way to access government services. Ms. Clarke suggested that, when governments subcontract private actors to deliver services, they must thoroughly define what data can be collected and how this data can be used and monetized.[135]

Ms. Clarke said that the government should look into the issues related to data management and think about how data should be combined, whether citizens really want the government to communicate with them directly and how they want government departments to be able to access their data. In her opinion, these issues raise questions not only about privacy, but also about the "need to maybe develop entirely new regimes, not necessarily in legislation, but in principles of data use."[136]

Mr. Roy said that there are imperfections and challenges in working with private actors, but he believes that working with the most sophisticated technology companies in the world is the right decision when it comes to digital government services, because these companies have the security capacities to enshrine privacy. He also said that the private sector should participate in the discussion around privacy, but that the government must

133 ETHI, *Evidence*, 1st Session, 42nd Parliament, 7 February 2019, 1610 (Amanda Clarke).

134 Ibid., 1635.

135 Ibid., 1540.

136 Ibid., 1640.

ensure that there is robust accountability for how companies partake in public infrastructure and what the implications are.[137]

Mr. Benay said that lessons were learned from problems related to the Phoenix system and that his organization, within the scope of its procurement activities, is conducting user expos across the country, letting users test various technologies and getting their feedback. Mr. Benay believes that making users central to the process has led to improvements in the decision-making mechanism to better meet the needs of human resources and pay administrators, as well as the everyday public servant. He believes that all the relevant stakeholders are involved in procurement, which is based on the principles of privacy by design.[138]

Mr. Benay also insisted that he is trying to move away from the traditional procurement process by working with vendors at every gate installed throughout the process in order to design it.[139]

According to Michael Fekete, Partner with Osler, Hoskin & Harcourt LLP and Co-Chair, Legal Affairs Forum, Information Technology Association of Canada, the Government of Canada is lagging behind other governments in terms of cloud adoption because data classifications in Canada are matched with security requirements that are incompatible with cloud services. For Canada to catch up, Mr. Fekete said that it could draw insight from international best practices, such as the United Kingdom's G-Cloud, which is considered a model for digital government and cloud adoption. Mr. Fekete added that the success of G-Cloud is due to strategic policy changes to support the implementation of cloud-based technology, including:

- a simplified data classification regime;
- non-prescriptive security requirements;
- accountability for decisions to procure bespoke solutions; and
- a willingness to accept a supplier's contract with a "wrapper" of government terms.[140]

---

137 Ibid., 1655 (Jeffrey Roy).

138 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1605 (Alex Benay).

139 Ibid.

140 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2019, 1545 (Michael Fekete, Partner, Technology, National Innovation Leader, Osler, Hoskin & Harcourt LLP, Information Technology Association of Canada).

Mr. Fekete said that government departments and agencies in the United Kingdom are required to evaluate a cloud service against 14 cloud security principles, which serve as a checklist for effective security safeguards—without prescribing how a cloud provider needs to demonstrate compliance.[141]

According to Mr. Boysen, it is not a good idea to give one company a monopoly on the procurement of digital government services and an open scheme with multiple providers is needed.[142]

C. Cybersecurity and digital government services

On the topic of cybersecurity and digital government services, Mr. Therrien said that technological systems are vulnerable to breaches and that the government should be legally required to apply strong technological safeguards, such as blockchain or encryption.[143]

From a different point of view, Mr. Vickery said that he is wary of blockchain technology because it is not mature enough, in his view. He added that, according to him, databases should not speak the same language, communicate with each other or pool their data together. Instead, there should be a "translator" in the middle. The government could then decide that the translator is not always available, which would alleviate concerns that ill-intentioned individuals could gain access to a given data bank and thereby to all of the others.[144]

Mr. Vickery said that it is always best to assume there has been a breach and to make the system so segmented and resilient that even if there is a breach, it is possible to rapidly detect it and ensure that the damage is minimal.[145]

He also said that the banking sector is not a bad choice to entrust with the creation and maintenance of a system to collect and protect data from digital government services and guarantee its security. Banks are highly regulated and accustomed to very intense audits, keeping paper trails, and doing everything by the book. However, Mr. Vickery recommended caution about how the data will be allowed to be used in other ways,

141 Ibid.

142 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 February 2019, 1600 (Andre Boysen).

143 ETHI, *Evidence*, 1st Session, 42nd Parliament, 31 January 2019, 1555 (Daniel Therrien).

144 ETHI, *Evidence*, 1st Session, 42nd Parliament, 5 February 2019, 1600 (Chris Vickery).

145 Ibid., 1655.

adding that clear lines must be drawn with banks when using their expertise and infrastructure.[146]

Mr. Benay said that it is paramount to ensure that digital government services are secure by design, adding that security has been central to every major digital project moving forward in the government over the last 12 months. However, he does not support putting all government information into one big system or data pool.[147]

Ruth Naylor, Executive Director, Information and Privacy Policy Division, Chief Information Officer Branch, said that, under Treasury Board policies, government institutions are required to report privacy breaches that are material in nature to the OPC and the Treasury Board Secretariat. She added that her organization works quite closely with the OPC to compare notes on those reports, and that the Treasury Board Secretariat has a range of tools available to institutions to help them identify, manage and report privacy breaches.[148]

Ms. Naylor said that her organization and the OPC are developing a two-year action plan, which aims to increase awareness about the nature of personal information, what a breach is and how to report one. Her efforts are focused on the IT and security community and making sure they have the instinct to recognize when personal information is involved.[149]

André Leduc, Vice-President, Government Relations and Policy, Information Technology Association of Canada, said that his organization believes that if the government "adopt[s] a balanced approach and [adjusts] elements of its current data classification system and security framework, these two objectives [will be] both compatible and interdependent."[150]

On the topic of 5G technology, Mr. Leduc said that the current networks will not be able to manage the volume of data generated by all the sensors in smart cities, on roads, in

146 Ibid., 1620.

147 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1605 (Alex Benay).

148 Ibid., 1610 (Ruth Naylor, Executive Director, Information and Privacy Policy Division, Chief Information Officer Branch).

149 Ibid.

150 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2019, 1540 (André Leduc, Vice-President, Government Relations and Policy, Information Technology Association of Canada).

automated cars, and so on.[151] He added that, in terms of adopting new technology, Canada ranks third in the world, according to the United Nations.[152]

Mr. Fekete said that the Government of Canada's 2018 cloud adoption strategy requires government departments and agencies to follow a structured risk management approach that takes into account the inclusion of cloud services in their IT services.[153]

M. Anthony, believes there is a global skills shortage in the core capabilities needed to securely govern, develop, test, deploy and maintain complex software systems, adding that this comment applies to the global digital transformation.[154]

Ms. McIver expressed a unique perspective on the use that can be made of the data following a security breach:

> We have to get to a point where we make the data almost useless. What is important is the validation that comes with the data. Therefore, if there is an attack—a social engineering attack or otherwise—where the data is collected by the attackers and somehow attempted to be invoked into the system, it's rejected because it's not coming from a validated source.[155]

Angelina Mason, General Counsel and Vice-President of the CBA, said that education is a significant part of the fight against cyber fraud: "[w]e educate and let consumers know the risks out there. Also, it's a sharing of information to find technological ways to block certain types of communications."[156]

Ms. Mason also said that having data outside Canada is a common practice for financial institutions and companies. She added that federal privacy legislation requires that if data is to be housed outside of Canada, it must be kept as secure as if it were in Canada, and consumers must be notified.[157]

---

151 Ibid., 1625.

152 Ibid., 1630.

153 Ibid., 1545 (Michael Fekete). See Government of Canada White Paper: Data sovereignty and Public Cloud.

154 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 February 2019, 1535 (Matthew Anthony).

155 Ibid., 1630 (Rene McIver, Chief Security Officer, SecureKey Technologies Inc.).

156 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 April 2019, 1600 (Angelina Mason, General Counsel and Vice-President, Canadian Bankers Association).

157 Ibid., 1605.

In terms of the role banks play, John O'Brien, Director, Security and Engineering Reliability, Canadian Digital Service, said the following:

> I don't actually know how banks secure their systems. For me to say that I think they are in the best position to protect Canadian security would be kind of out of place. I would love it if they would be more open and honest about that, just like I would love it if Google and Facebook and all these companies would be very open and honest about how they do security things. At that point, we could all collectively bring up our security postures, and I think Canadian citizens would be a lot more trusting of all of the parts.[158]

D. Waterfront Toronto's Quayside project

As part of its study on digital government services, the Committee examined the Quayside project, which aims to create a smart city in the Toronto waterfront neighbourhood. Sidewalk Labs (SWL), an organization owned by Alphabet (of which Google is a subsidiary) has been mandated to prepare a proposal for what this smart city could look like for Waterfront Toronto, the entity that manages the revitalization of the waterfront neighbourhood where the smart city project would be implemented. This project and the challenges that it presents offered the Committee a concrete example of the implementation of digital municipal services.

However, the project was strongly criticized by some witnesses who appeared before the Committee as part of the International Grand Committee on Big Data, Privacy and Democracy held from 27-29 May 2019.

Shoshana Zuboff, professor emerita of the Harvard Business School and *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* explained the following:

> It is auspicious that we are meeting tonight in this beautiful country of Canada, because right now, the front line of this war between surveillance capitalism and democracy is being waged in Canada, specifically in the city of Toronto. Surveillance capitalism began with your online browsing and moved to everything that you do in the real world. Through Facebook's online massive-scale contagion experiments and Google-incubated Pokémon GO, it experimented with population-level herding, tuning and behaviour modification.
>
> Those skills, by the way, have now been integrated into Google's smart city application called Waze. But the real apple here, the real prize, is the smart city itself. This is where surveillance capitalism wants to prove that it can substitute computational rule, which

158 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 February 2019, 1635 (John O'Brien, Director, Security and Engineering Reliability, Canadian Digital Service).

> is, after all, a form of absolutist tyranny, for the messiness and beauty of municipal governance and democratic contest.
>
> The frontier is the smart city. If it can conquer the smart city, it can conquer democratic society. Right now, the war is being waged in Toronto. If Canada gives Google, that is, Alphabet—Sidewalk Labs now goes out of its way to claim that it is not Google—Toronto, a blow will be struck against the future possibilities of a democratic society in the 21st century.[159]

Jim Balsillie, founder and former co-CEO of Research in Motion and Chair of the Centre for International states that "Canadians are currently in a historic battle for the future of our democracy with a charade called Sidewalk Toronto."[160] Finally, Roger McNamee, former mentor of Mark Zuckerberg and author of Zucked, affirmed:

> I wouldn't let them within 100 miles of Toronto. The fundamental issue here is one of self-governance and self-determination. I just don't believe that any business—not Google, not anybody—should be in the business of operating our public spaces and our civic infrastructure. There is a limit to what you can do with a public-private partnership, and that is way over the line.
>
> …
>
> The observation I would make is that I am still cautious about the gathering of the data in the first place. I believe that the underlying issues relative to surveillance create too many temptations for people. At the moment, it's way, way too difficult to monitor what they're doing with the data once it's collected. I believe that all of these things require, to use an old government phrase, dramatically more study before we move forward.[161]

Representatives from Waterfront Toronto and SWL appeared before the Committee. They indicated, for their part, that they have a commitment to the protection of personal information. They also explained some of the measures they intend to take as part of the Quayside project to ensure the protection of the data collected.

Kristina Verner, Vice-President, Innovation, Sustainability and Prosperity with Waterfront Toronto, argued that while Canadian privacy laws have proven remarkably effective relative to the rest of the world, they have to keep up with technological changes. She said that with respect to the Quayside project, Waterfront Toronto will protect the right to privacy beyond the letter of the law and that the project reflects Canadian values on

---

159 ETHI, *Evidence*, 1st Session, 42nd Parliament, 27 May 2019, 1950 and 1955 (Shoshana Zuboff).

160 ETHI, *Evidence*, 1st Session, 42nd Parliament, 28 May 2019, 0835 (Jim Balsillie).

161 Ibid., 0930 (Roger McNamee).

privacy.[162] With respect to the protection of personal information in this smart city project, she explained that the following measures will be taken by Waterfront Toronto:

1. complying with all existing legislative and regulatory requirements for the project and adhering to the principles of privacy by design (the project would only be approved if it adheres to these principles);

2. awarding no preferential treatment to any Alphabet company, including Google, that would allow the sharing or use of personal data;

3. making it impossible to use data for advertising purposes without express consent;

4. ensuring that personal information will be de-identified at source, unless express consent is knowingly and explicitly given for a specific purpose;

5. minimizing data collection so that only the data needed and identified for limited and specified purposes would be collected; and

6. pledging that data collected for the Quayside project will be stored in Canada.[163]

Ms. Verner also reaffirmed Waterfront Toronto's commitment to de-identify data at source (at the point of collection or the initial point of storage or processing). As for the smart city's information sensors, she said that Waterfront Toronto's proposition was that, immediately upon collection, individuals' pictures would be converted into shapes that are vague enough so that features such as gender, age and difference of ability would be indistinguishable. These shapes would then be converted into numbers, algorithms and statistics, implying that there would be less privacy risks.[164]

Ms. Verner added, however, that if all data is open by default, some small companies in Canada may be disadvantaged and this issue should be addressed in the upcoming stages.[165]

---

162 ETHI, *Evidence*, 1st Session, 42nd Parliament, 21 February 2019, 1535 (Kristina Verner, Vice-President, Innovation, Sustainability and Prosperity, Waterfront Toronto).

163 Ibid.

164 Ibid., 1555.

165 Ibid., 1640.

As for the question of civic data trust, which has been proposed in the context of the Quayside project, Ms. Verner said that civic data trusts are a potential governance model, but that Waterfront Toronto intends to study other models once the company has a better idea of what it is seeking. She added that Waterfront Toronto does not wish to play the role of data keeper or digital overseer of the project.[166]

With respect to the data collected from the physical environment by cameras and sensors, SWL suggested creating an independent organization to oversee the collection and use of "urban data" and doing so "in a way that protects the public interest while encouraging innovation."[167]

Dan Doctoroff, the Chief Executive Officer of SWL, stated that Sidewalk Labs wishes that urban data be made publicly available and de-identified by default. However, he added a caveat: there are certain situations where SWL could make the case that it is impossible to get the data's full value without further restricting access, which would be done by a civic data trust in consultation with privacy regulators because it goes beyond the company's responsibility.[168]

Mr. Doctoroff also said that:

> Consistent with Canadian laws and values on privacy, we made early commitments with regard to responsible data use, including to the principles of privacy by design, to de-identification and data minimization and to not selling personal data from this project or using it for advertising purposes.[169]

When asked about his business model and how SWL intends to make money, Mr. Doctoroff said that SWL has no interest in monetizing personal information.[170]

The Committee also heard the testimony of Brian Kelcey, Vice-President, Public Affairs, Toronto Region Board of Trade. Mr. Kelcey stated that the process agreed to by

166 Ibid., 1645.

167 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 April 2019, 1540 (Dan Doctoroff, Chief Executive Officer, Sidewalk Labs)

168 Ibid., 1645.

169 Ibid., 1540.

170 Ibid., 1610.

Waterfront Toronto and SWL should proceed, and that the outcome should be based on the merits or demerits of whatever SWL presents in its development plan.[171]

Mr. Kelcey presented the key recommendations of his organization's report, *BiblioTech*, released in January 2019, and addressing the issue of data governance of the data that would be collected in the context of the Quayside project:

- data regulation related to the Quayside project should be handled by a third-party organization, not the project's proponents or participants;
- any public realm data collected in the city of Toronto should, by law and regulation, be held by a public data hub or a public data host or trust;
- a good potential host for that hub would be the Toronto Public Library;
- enforcement of those rules should fall within the purview of the Information and Privacy Commissioner of Ontario;
- those rules should be toughened as appropriate, and that the Commissioner should have authority to investigate breaches of rules of that data hub if needed;
- the Toronto Public Library should model any effort to capture intellectual property value from this data on the approaches used at university and post-secondary tech transfer offices; and
- revenue should be used to make the hub self-sustaining, even if commercialization of data was limited.[172]

Mr. Kelcey believes that there is a consensus that public realm data must be regulated by governments or agencies if SWL wishes to commercialize data from sensors at Quayside.[173] Once collected, the public realm data "should be held independently by an external authority, be that the government, a trust or some suitable agency."[174]

171 ETHI, *Evidence*, 1st Session, 42nd Parliament, 9 April 2019, 1605 (Brian Kelcey, Vice-President, Public Affairs, Toronto Region Board of Trade).

172 Ibid.

173 Ibid.

174 Ibid., 1610.

Based on the evidence heard with respect to the Quayside project, the Committee recommends that:

Recommendation 8 on the establishment of guidelines and principles for smart city projects:

That the Government of Canada, in partnership with provincial, municipal and Indigenous governments, establish guiding principles relating to privacy, cybersecurity and digital literacy in smart city projects.

CONCLUSION

The Committee found in its study that several advances in digital government services are underway within the federal government.

However, several witnesses raised potential solutions that would enable the Government of Canada to ensure that the deployment of digital services is done in an efficient and successful manner.

In light of all the evidence heard, the Committee takes some of these potential solutions and presents them in the form of recommendations. It also wishes to emphasize the importance of ensuring that the shift to digital government services does not come at the expense of protecting the privacy of Canadians.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the Committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the Committee's webpage for this study.

Organizations and Individuals	Date	Meeting
E-Governance Academy	2018/03/22	96
Liia Hänni, Senior Expert		
Raul Rikk, Programme Director National Cyber Security		
As an individual	2018/03/27	97
Jerry Fishenden, Technologist and Government Advisor		
As individuals	2019/01/29	132
Ann Cavoukian, Privacy by Design Centre of Excellence, Ryerson University		
Michael Geist, Canada Research Chair in Internet and E-Commerce Law Faculty of Law, University of Ottawa		
Office of the Privacy Commissioner of Canada	2019/01/31	133
Lara Ives, Executive Director Policy, Research and Parliamentary Affairs Directorate		
Gregory Smolynec, Deputy Commissioner Policy and Promotion Sector		
Daniel Therrien, Privacy Commissioner of Canada		
As individuals	2019/02/05	134
David Carroll, Associate Professor Parsons School of Design, The New School		
Chris Vickery, Director of Cyber Risk Research UpGuard		
Digital Content Next	2019/02/05	134
Jason Kint, Chief Executive Officer		

Organizations and Individuals	Date	Meeting
As individuals	2019/02/07	135
Amanda Clarke, Assistant Professor and Public Affairs Research Excellence Chair School of Public Policy and Administration, Carleton University		
David Eaves, Lecturer in Public Policy Digital HKS, Harvard Kennedy School		
As an individual	2019/02/07	135
Jeffrey Roy, Professor School of Public Administration, Dalhousie University		
Treasury Board Secretariat	2019/02/19	136
Alex Benay, Chief Information Officer of the Government of Canada		
Ruth Naylor, Executive Director Information and Privacy Policy Division, Chief Information Officer Branch		
John O'Brien, Director Security and Engineering Reliability, Canadian Digital Service		
Aaron Snow, Chief Executive Officer Canadian Digital Service		
Information Technology Association of Canada	2019/02/21	137
Michael Fekete, Partner Technology, National Innovation Leader, Osler, Hoskin & Harcourt LLP		
André Leduc, Vice-President Government Relations and Policy		
Waterfront Toronto	2019/02/21	137
Meg Davis, Chief Development Officer		
Kristina Verner, Vice-President Innovation, Sustainability and Prosperity		
Herjavec Group	2019/02/28	139
Matthew Anthony, Vice-President Security Remediation Services		
Ira Goldstein, Senior Vice-President Corporate Development		

Organizations and Individuals	Date	Meeting
SecureKey Technologies Inc.	2019/02/28	139
Andre Boysen, Chief Information Officer		
Rene McIver, Chief Security Officer		
Sidewalk Labs	2019/04/02	141
John Brodhead, Director of Policy and Strategy		
Dan Doctoroff, Chief Executive Officer		
Micah Lasher, Head of Policy and Communications		
Canadian Bankers Association	2019/04/04	142
Marina Mandal, Vice-President Banking Transformation and Strategy		
Angelina Mason, General Counsel and Vice-President		
Symcor Inc.	2019/04/04	142
Della Shea, Vice-President Privacy & Data Governance and Chief Privacy Officer		
Toronto Region Board of Trade	2019/04/09	143
Brian Kelcey, Vice-President Public Affairs		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the Committee related to this report. For more information, please consult the Committee's webpage for this study.

Di Lorenzo, Julie

Eaves, David

Rubin, Ken

Sack, Cybele

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 96, 97, 132 to 137, 139, 142 to 144, 149, 150, 156, 158 and 159) is tabled.

Respectfully submitted,

Bob Zimmer
Chair

Supplemental Report on Smart Cities and Democratic Rights

New Democratic Party

Introduction

In the course of the Committee's study into the Privacy of Digital Government Services, the Committee heard evidence on the related issue of the controversial "smart city" project being developed by the Alphabet subsidiary Sidewalk Labs on Toronto's waterfront.

The project is a response to a Request for Proposals from Waterfront Toronto, a corporation jointly established by the Governments of Canada, Ontario and Toronto and responsible for the development of the city's waterfront, seeking an Innovation and Funding Partner to develop a 12-acre plot of land called Quayside.

Since Waterfront's joint announcement with Sidewalk Labs in October 2017, which additionally included its parent company Alphabet, the Government of Canada, the Government of Ontario and the City of Toronto, the "smart city" project has been dogged by controversy, from a report from the Auditor General of Ontario that raised serious questions about the project to a spate of resignations from advisory positions within both Sidewalk Labs and Waterfront Toronto.

The concerns raised include the protection of residents' privacy, the process through which Sidewalk Labs was granted the opportunity to develop a Master Innovation and Development Plan and the surveillance capitalism business model of Sidewalk parent company Alphabet.

It is now facing serious resistance from a coalition of Torontonians organizing as Block Sidewalk.

New Democrats recommend that:

1. The Government of Canada suspend engagement with and commitment to Sidewalk Labs until a final, detailed plan is submitted to Waterfront Toronto, the City of Toronto, the Province of Ontario and the federal government.
2. Any "smart city" projects in Canada begin with a public consultation of residents' needs and desires;
3. Be continuously oriented towards addressing these real needs and desires;
4. Include citizen input and design as thoroughly as possible;
5. Any "smart city" project ultimately cannot be deployed to serve a surveillance capitalism business model.

Concerns with Process – Request for Proposals

The Quayside development has faced serious questions from the beginning about the process used to select Sidewalk Labs as the potential innovation and funding partner awarded the opportunity to present Waterfront Toronto with a Master Innovation and Development Plan.

Waterfront Toronto's original request for proposals (RFP), entitled "Request for Proposals: Innovation and Funding Partner for the Quayside Development Opportunity" was issued on March 17, 2017, and specified a submission deadline of April 27, 2017.[1] This is six weeks, or 30 business days.

A "smart city" project is an enormous undertaking, and indeed, this project would be the first of its kind and scope in Canada. It involves complicated questions about data collection and privacy, governance and democratic accountability, intellectual property, and land use, to name a few. As the Auditor General of Ontario noted in her 2018 audit of Waterfront Toronto, "respondents were given six weeks to respond to a complex request for proposal – in comparison to 10 weeks previously been given to respondents for public art projects in the West Don Lands."[2] The Auditor General's Report further noted that Waterfront Toronto had previously had RFP submission periods of "11 weeks for a construction manager for Port Lands flood protection and 25 weeks for a developer to lead the construction of a single office building."[3] She ultimately concluded that "six weeks was not enough time for respondents to respond to [the] RFP."[4]

On the February 21st, 2019, meeting of the Committee, Waterfront Toronto's Chief Development Officer, Meg Davis, told the Committee that the RFP period was 159 days. Sidewalk Labs' Chief Executive Officer, Dan Doctoroff, also told the Committee this during his appearance before the Committee on April 2nd, 2019.

Despite these claims, Waterfront Toronto did not apparently raise this matter with the Auditor General of Ontario in the course of her value-for-money audit of the organization, and she duly reported that the RFP period was only six weeks, as noted above. Likewise, Waterfront Toronto did not note their objections to this interpretation of events in their formal responses to the Auditor General included in her Report. A statement from the interim CEO of Waterfront Toronto, Michael Nobrega, issued in response to the Auditor General's Report, also made no reference to the brevity of the RFP and made no attempt to contest the Auditor General's determination that the submission period was six weeks long.[5]

Mr. Kent, a Conservative member of this Committee, raised in questions to Mr. Doctoroff that other parties submitting responses to the RFP were aware only of the 30-day period specified in Quayside's original RFP. This view was not contradicted by Mr. Doctoroff.

New Democrats believe that Waterfront Toronto and Sidewalk Labs' insistence that the RFP period was 159 days is in contradiction to their own documents, the understanding of other respondents, the

---

[1] Waterfront Toronto, "Quayside Request for Proposals: Innovation and Funding Partner for the Quayside Development Opportunity," March 17, 2017, page 1.
https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/3f21abe9-a5bb-4665-8cd3-322e1e13811f/Waterfront+Toronto+-+RFP+No.+2017-13.pdf?MOD=AJPERES&CACHEID=3f21abe9-a5bb-4665-8cd3-322e1e13811f

[2] Auditor General of Ontario, 2018 Annual Report, "Chapter 3.15: Waterfront Toronto," 651.

[3] Auditor General, "Waterfront Toronto," 690.

[4] Ibid., 690.

[5] Waterfront Toronto, "Statement by Waterfront Toronto Interim CEO Michael Nobrega Regarding the Report of Ontario's Auditor General," December 5, 2018.
https://waterfrontoronto.ca/nbe/portal/waterfront/Home/waterfronthome/newsroom/newsarchive/news/2018/december/statement+from+waterfront+toronto+regarding+ontario+auditor+general+report

Auditor General of Ontario's report, and contemporary coverage of the process in the media, and is not credible.

The Auditor General's critical role of performing detailed oversight is indispensable in our system of government. It is not enough to casually contradict a report of the Auditor General, particularly after the fact as Waterfront Toronto and Sidewalk Labs both did. This has undermined our confidence in the project and should trouble Torontonians and Canadians.

Given the power and scope of Alphabet as a corporation, and the oft-noted public concerns about the technological and governance aspects of this project, these contradictions are not acceptable.

Further, given the complexities surrounding "smart city" projects noted above and given that Sidewalk Labs noted in its submissions to the Auditor General that they see their commitment to Toronto "as a twenty-plus year undertaking," the short RFP was in itself inappropriate.

New Democrats believe that any "smart city" project should involve deep and proactive consultation with residents, a lengthy period to develop plans and respond to concerns in the public sphere, and a thorough understanding on the part of residents, civic officials and the public precisely of what is being agreed to at every step of the process before deals are signed.

Finally, it is unclear to New Democrats that Waterfront Toronto, which per s. 13(3) of its enabling legislation, the *Toronto Waterfront Revitalization Corporation Act*, must be finally wound up by order of the Lieutenant Governor of Ontario-in-Council no later than 2028, is an appropriate body to be entering the public into a generational commitment such as a long-term "smart city" project with so many unknowns.

Concerns with Process – Approval of Framework Agreement

In her Report, the Auditor General noted that Waterfront Toronto "did not adequately consult with any levels of government regarding the Sidewalk Labs project." Instead of consultation with relevant provincial ministries and federal and municipal departments, she said, "this was being discussed at a senior political level."[6] She further notes that "the Board felt it was being 'urged – strongly' by the federal and provincial governments to approve and authorize the Framework Agreement with Sidewalk Labs as soon as possible," that the Board itself only had one day to consider and approve the agreement, and that an announcement of the approved agreement with the Prime Minister, the Premier of Ontario, the Mayor of Toronto and the Executive Chairman of Alphabet had already been scheduled for October 17th on October 12th, "the day before the Board received the final Framework Agreement for review and approval."[7]

Though the Auditor General did not provide more detail on the nature of these discussions at a senior political level, she also found that the 2017 RFP seeking an innovation and funding partner was not consistent with the objectives and priorities laid out in Waterfront Toronto's 2014-2023 Strategic Plan, and that Waterfront Toronto's own Intergovernmental Steering Committee rebuked the organization in

[6] Auditor General, "Waterfront Toronto," 652.
[7] Ibid., 690-1.

a November 2017 meeting for not providing adequate time to Waterfront Toronto's Board in advance of major decisions.[8]

In her submission to our Committee, Ms. Julie Di Lorenzo, a past board member of Waterfront Toronto and the Chair of the Board's Investment and Real Estate Committee (IREC) who resigned over the organization's handling of the Sidewalk Toronto project, noted serious concerns about the approval process for the original October 2017 framework agreement and inaccuracies in Waterfront Toronto's testimony to our Committee about the same.

In her letter, she says that she dissented on a vote to approve the framework agreement because IREC, which Ms. Davis of Waterfront Toronto claimed before our Committee on February 21st, "[had] reviewed every clause and every comma and [had] been helping the team negotiate," was only provided with a copy of the agreement four business days prior to the meeting of the full Board.[9] The Board approved the agreement without IREC's recommendation, and as Ms. Di Lorenzo notes, in normal proceedings, "if the lead subcommittee chair opposes a motion, that is sufficient grounds to suspend further action until the concerns at least permit a fulsome consideration of that chair's concerns. That the Chair of the Investment and Real Estate Committee dissented on an investment and real estate project vote is extraordinary."[10]

Ms. Di Lorenzo also stated that Ms. Davis' claim before our Committee that there was only one vote against the framework agreement at the meeting of the full board on October 16th was, while technically accurate, not a fair characterization. Ms. Di Lorenzo states that there were two absent members who did not provide a vote by proxy, and another member of the board abstained. As she puts it, "the lead subcommittee chair on the board dissented, two members were absent, and one Board Member abstained. Contrary to Ms. Davis' characterization of the meeting, in fact, the board vote on the motion reflected a distinct *lack* of consensus by Waterfront Toronto, which was clearly divided and uninformed over such a historic, consequential agreement with no reasonable time to review and contemplate the impacts of said agreement."[11]

Ms. Davis told our Committee that the Investment and Real Estate Committee had had several meetings about the agreement in advance of its unveiling, but Ms. Di Lorenzo calls this "misleading."[12] She states that in her experience as chair of that committee that "those meetings were not about the actual Framework Agreement since the actual agreement was not available until Thanksgiving weekend 2017. The meetings of the IREC Committee prior to the Thanksgiving weekend 2017 were about various Waterfront Toronto business items such as affordable housing, high level briefings on the potential agreement, but not the Framework Agreement itself."[13] This is corroborated by the Auditor General's report, which states that the "Committee received an overview of the principles and draft terms of the

[8] Ibid., 688-9.
[9] Ms. Meg Davis, Oral Testimony to the Standing Committee on Access to Information, Privacy and Ethics, February 21, 2019.
[10] Julie Di Lorenzo, "Brief to the Standing Committee on Access to Information, Privacy and Ethics," May 9, 2019, page 2. https://www.ourcommons.ca/Content/Committee/421/ETHI/Brief/BR10470671/br-external/DiLorenzoJulie-e.pdf
[11] Di Lorenzo, "Brief," 2.
[12] Ibid., 4.
[13] Ibid., 4.

Framework Agreement about one month prior to the submission of the agreement to Board for approval."[14]

As noted above, the Sidewalk Labs "smart city" project is a generational commitment for the City of Toronto and for Canadians. The procedural irregularities in Waterfront Toronto's approval process for the Framework Agreement and the inconsistencies in their testimony before our Committee have served to undermine New Democrats' confidence in this project.

Surveillance Capitalism and Democracy

This Committee recently heard a great deal of evidence from leading experts on what is increasingly often called surveillance capitalism and the risks it poses to citizens' democratic rights, both through a business model that is fundamentally an affront to human autonomy and the new institutional and market power of its leading practitioners, which include companies such as Alphabet, Facebook and Amazon.

Dr. Shoshana Zuboff, professor emerita at the Harvard Business School and the author of *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* defined surveillance capitalism before our Committee as "a comprehensive, systemic economic logic that is unprecedented in our experience," in that it "claims private human experience for the market dynamic." [15]

In previous modes of capitalism, Dr. Zuboff argues, capital took "something that exists outside the marketplace and [brought] it into the market dynamic for production and sale. Industrial capitalism famously claimed nature for the market dynamic, to be reborn as land or real estate that could be sold or purchased." Surveillance capitalism, she argues, "claims private human experience for the market dynamic." [16]

Dr. Zuboff further elaborated that under surveillance capitalism, "private human experience is repurposed as free raw material. These raw material[s] are rendered as behavioural data. Some of these behavioural data are certainly fed back into product and service improvement, but the rest are declared a behavioural surplus identified for their rich predictive value."

This "behavioural surplus" is, through the application of machine learning technology, turned into what Dr. Zuboff calls a "prediction product," which is "sold into a new kind of marketplace that trades exclusively in human futures. The first name of this marketplace was online targeted advertising. The human predictions that were sold in those markets were called click-through rates. Zoom out only a tiny bit and what you understand is that the click-through rate is simply a fragment of a prediction of a human future."

These are ultimately used by the platforms able to leverage economies of scope and scale to offer refined predictive and even determinative (i.e. behavioural modification) services to their customers.[17]

---

[14] Auditor General, "Waterfront Toronto," 690.
[15] Dr. Shoshana Zuboff, Oral Testimony to the Standing Committee on Access to Information, Privacy and Ethics, May 28, 2019.
[16] Zuboff, Oral Testimony, May 28, 2019.
[17] Ibid.

Ultimately, Dr. Zuboff argued, the model's objective is "to have surveillance capitalism's computational analysis which favours its own commercial outcomes replace democracy and governance as we know it." [18] Mr. Roger McNamee, an early Facebook investor and expert on Silicon Valley, corroborated this, saying that for surveillance capitalists, "behavioural manipulation is the goal."[19]

Dr. Zuboff suggested that the way for legislators and regulators to address the harms caused by surveillance capitalism is to "devise strategies that interrupt and in many cases outlaw surveillance capitalism's foundational mechanisms. This includes the unilateral taking of private human experience as a free source of raw material and its translation into data. It includes the extreme information asymmetries necessary for predicting human behaviour. It includes the manufacture of computational prediction products based on the unilateral and secret capture of human experience."[20]

On smart cities, Dr. Zuboff said that "The frontier [of surveillance capitalism] is the smart city. If it can conquer the smart city, it can conquer democratic society. Right now, the war is being waged in Toronto. If Canada gives Google, that is, Alphabet—Sidewalk Labs now goes out of its way to claim that it is not Google—Toronto, a blow will be struck against the future possibilities of a democratic society in the 21st century." On Sidewalk specifically, Dr. Zuboff further described it as "a reincarnation of a kind of absolutist tyranny that we thought we had left behind us in the 18th century, now served with cappuccino and draped in ones and zeroes," through a "direct bypassing of democracy in order to impose their vision, which ultimately is aimed at their own narrow commercial purposes."[21]

Mr. Jim Balsillie, the founder and former CEO of Research in Motion, also told the committee that "technology is disrupting governance, and if left unchecked could render liberal democracy obsolete. … Technology is becoming the new fourth estate and our system of checks and balances. This makes technology co-equal with the executive, the legislative and the judiciary." Mr. Balsillie further stated specifically that "Canadians are currently in a historic battle for the future of our democracy with a charade called Sidewalk Toronto."[22]

Mr. McNamee said specifically of Sidewalk Toronto that he "wouldn't let them within 100 miles of Toronto. The fundamental issue here is one of self-governance and self-determination. I just don't believe that any business—not Google, not anybody—should be in the business of operating our public spaces and our civic infrastructure. There is a limit to what you can do with a public-private partnership, and that is way over the line."

He further stated that he is "still cautious about the gathering of the data [in a smart city] in the first place. I believe that the underlying issues relative to surveillance create too many temptations for people, and at the moment it is way too difficult to monitor what they're doing with the data once it's

[18] Ibid.
[19] Mr. Roger McNamee, Oral Testimony to the Standing Committee on Access to Information, Privacy and Ethics, May 28, 2019.
[20] Zuboff, Oral Testimony, May 28, 2019.
[21] Ibid.
[22] Mr. Jim Balsillie, Oral Testimony to the Standing Committee on Access to Information, Privacy and Ethics, May 28, 2019.

collected." Mr. McNamee also recommended looking at Barcelona's ongoing "smart city" project as a potential alternative model.[23]

New Democrats believe that surveillance capitalism as a business model poses a serious risk to democratic government and human autonomy. Further, they take the specific concerns of Dr. Zuboff, Mr. McNamee and Mr. Balsillie about the uncertainties and risks of the Sidewalk Toronto project seriously and believe that Torontonians are well within their rights to demand better for themselves and their community.

The services and conveniences that "smart city" visions hold out are not themselves inimical New Democrats believe that a responsible "smart city" project built democratically from the ground up has great promise.

The surveillance capitalism business model of Sidewalk's parent company Alphabet, however, as well as the concerns over process detailed above, leave them with no choice but to say that the Government of Canada, the Government of Ontario and the City of Toronto should be very skeptical of this project and take great care before making any long-term commitments on their citizens' behalf.

[23] McNamee, Oral Testimony, May 28, 2019.