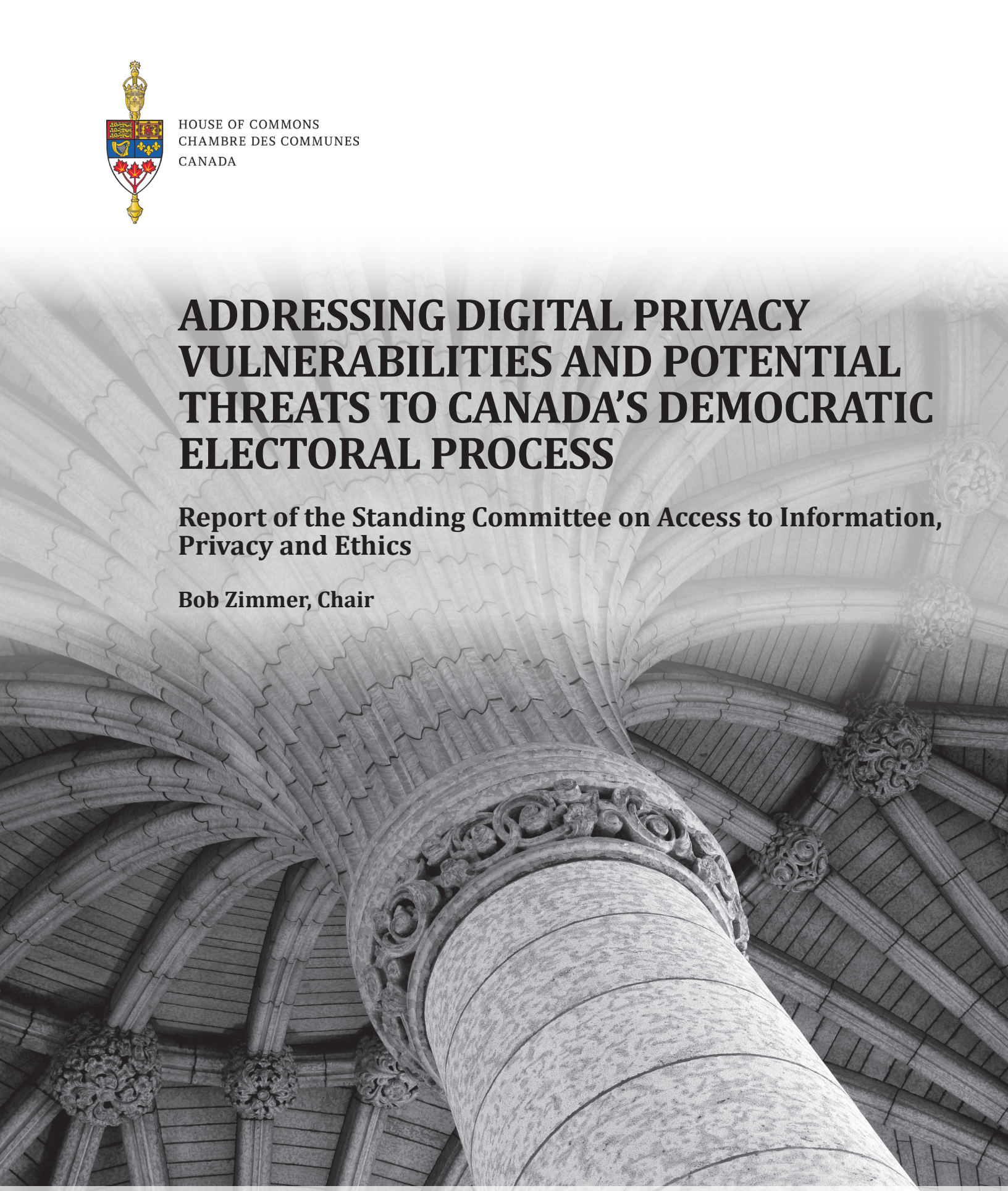
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

ADDRESSING DIGITAL PRIVACY VULNERABILITIES AND POTENTIAL THREATS TO CANADA'S DEMOCRATIC ELECTORAL PROCESS

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

Bob Zimmer, Chair



JUNE 2018
42nd PARLIAMENT, 1st SESSION

ADDRESSING DIGITAL PRIVACY VULNERABILITIES AND POTENTIAL THREATS TO CANADA'S DEMOCRATIC ELECTORAL PROCESS

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

Bob Zimmer
Chair

JUNE 2018

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

Joyce Murray*

Michel Picard

Raj Saini

Anita Vandenbeld

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Ziad Aboultaif

Hon. Maxime Bernier

Alexandre Boulerice

Kerry Diotte

Andy Fillmore

Michael Levitt

Wayne Long

Brian Masse

Kelly McCauley

Alistair MacGregor

Eva Nassif

Jean-Claude Poissant

Terry Sheehan

Marwan Tabbara

Mark Warawa

* Non-voting member, pursuant to Standing Order 104(5)

CLERK OF THE COMMITTEE

Jean-Denis Kusion

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Alexandra Savoie

Maxime-Olivier Thibodeau

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

SIXTEENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*h*)(vii) and the motion adopted on Thursday, March 22, 2018, the Committee has studied the breach of personal information involving Cambridge Analytica and Facebook and has agreed to report the following:

PREAMBLE

In late March, the Standing Committee on Access to Information, Privacy and Ethics began a study of the breach of personal information involving Cambridge Analytica and Facebook, and the broader privacy implications of platform monopolies, which play an outsized role in our daily lives.

The scandal has brought to light issues relating to mass data harvesting, the use of data for nefarious purposes, and the threats and challenges these questionable methods can create for democracies around the world.

The evidence that the Committee has heard so far gives rise to grave concerns that the Canadian democratic and electoral process is similarly vulnerable to improper acquisition and manipulation of personal data.

In the Committee's view and in light of the evidence heard thus far, it has become quite apparent that the government of Canada must urgently act in order to better protect the privacy of Canadians. It should:

- Strengthen the powers of the Office of the Privacy Commissioner, including the authority for the Privacy Commissioner to levy significant fines against organizations that contravene the *Personal Information Protection and Electronic Documents Act* (PIPEDA);

- Subject political activities to laws that protect Canadians' privacy;

- Regulate organizations and political actors to make them more transparent in their collection, use, and disclosure of personal information, including the use of any targeting and profiling techniques;

- Establish data sovereignty rules and requirements to ensure that Canadians' personal information is protected;

- Implement the recommendations of the Committee contained in its report on PIPEDA tabled in February 2018, in order to better align federal privacy legislation with the European Union *General Data Protection Regulation* (GDPR).

The Committee is conscious of the fact that it has only scratched the surface of the problem in this study and that many conclusions remain undrawn. It will continue this study with determination, in the hopes that it can contribute to a lasting solution for a global challenge.

In the meantime, this interim report provides insight into the work of the Committee and the evidence it has heard in the first few months of its study. Most importantly, it puts forward several preliminary recommendations for the consideration of the government of Canada.

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.

ADDRESSING DIGITAL PRIVACY VULNERABILITIES AND POTENTIAL THREATS TO CANADA'S DEMOCRATIC ELECTORAL PROCESS

INTRODUCTION

On 22 March 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) adopted a motion to conduct a study on the breach of personal information involving Cambridge Analytica and Facebook.[1] The motion reads as follows:

> That, in light of the large data breach perpetrated by Cambridge Analytica and unreported by Facebook for several years, the Committee conduct a study of the privacy implications of platform monopolies and possible national and international regulatory and legislative remedies to assure the privacy of citizens' data and the integrity of democratic and electoral processes across the globe; including testimony from the Cambridge Analytica whistleblower, Christopher Wylie, the Privacy Commissioner of Canada, Daniel Therrien, as well as directors and executives of large platform companies such as Facebook, Amazon and Google.

To date, the Committee has held nine public meetings on the subject between 27 March and 12 June 2018 during which it heard 16 witnesses, some of whom appeared twice.

The breach of personal information (the breach) revealed by Christopher Wylie (Mr. Wylie or the whistleblower) that exposed Cambridge Analytica, and by extension Facebook, sparked a national and international furor in recent months about the importance of protecting personal information and the risks of this information being used to influence the democratic and electoral process.

The breach led the Committee to conduct the current study. The United Kingdom Digital, Culture, Media and Sport Select Committee (the Digital Committee) also addressed the breach in its study on fake news.[2] In the United States, the breach was the focus of a joint full committee hearing by the Senate Committee on the Judiciary and the Senate Committee on Commerce, Science and Transportation, a hearing by the Energy and

1 House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Minutes of Proceedings*, 1st Session, 42nd Parliament, 22 March 2018.

2 Digital, Culture, Media and Sport Committee, Inquiries, Parliament 2017, *Fake news*.

Commerce Committee of the House of Representatives, and a second hearing by the Senate Committee on the Judiciary.[3]

In light of the above, the Committee would like to emphasize the exceptional nature of this study. Due to its interjurisdictional nature, the Committee is collaborating with the United Kingdom's Digital Committee, whose chair appeared before the Committee.[4] The Committee has also been in communications with its American counterparts from the aforementioned Senate and House of Representatives committees. It has also heard testimony from the United Kingdom Information Commissioner, as well as the Information and Privacy Commissioner for British Columbia. These interactions show an unprecedented level of mutual assistance between various jurisdictions to address the issue we are facing with monopoly platforms and their use for nefarious political purposes.

This study has raised important questions about the integrity of the democratic and election processes. It has led the Committee to consider legislative measures that could be implemented in Canada to ensure Canadians' personal information is better protected.

PART 1: THE BREACH OF PERSONAL INFORMATION

A. BACKGROUND

On 17 March 2018, *The New York Times* and the British newspaper *The Guardian* both published articles about the firm Cambridge Analytica. The story told in these two publications is based on the revelations of the whistleblower, Mr. Wylie, a former employee of Cambridge Analytica and its parent company, SCL Group (SCL). The story reveals how a breach of personal information by Cambridge Analytica gave it access to the profiles of more than 87 million Facebook users globally, a large proportion of those coming from users in the United States.[5] Facebook has since confirmed this figure.[6] It is alleged that this

3 United States Senate Committee on the Judiciary, Hearings, *Facebook, Social Media Privacy, and the Use and Abuse of Data*, 10 April 2018 (this was a joint full committee hearing with the Senate Committee on Commerce, Science, and transportation); Energy and Commerce Committee of the U.S. House of Representatives, Hearings, *Facebook: Transparency and Use of Consumer Data*, 11 April 2018; United States Senate Committee on the Judiciary, Hearings, *Cambridge Analytica and the Future of Data Privacy*, 16 May 2018.

4 ETHI, *Evidence*, 1st Session, 42nd Parliament, 3 May 2018 (Damian Collins, Chair, United Kingdom Digital, Culture, Media and Sport Select Committee).

5 *The New York Times*, "How Trump Consultants Exploited the Facebook Data of Millions", 17 March 2018; *The Guardian*, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", 17 March 2018.

6 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 April 2018, 0900 (Kevin Chan, Global Director and Head of Public Policy, Facebook Canada, and Robert Sherman, Deputy Chief Privacy Officer, Facebook Inc.).

personal information was used for nefarious political purposes. The breach also gave them access to the profiles of approximately 620,000 Canadian citizens.[7]

B. EVIDENCE FROM THE WHISTLEBLOWER AND KEY PARTIES IN THE BREACH OF PERSONAL INFORMATION INVOLVING CAMBRIDGE ANALYTICA AND FACEBOOK

1. Christopher Wylie

Mr. Wylie appeared before the Committee on 29 May 2018. He informed the Committee that he was hired in July 2013 by SCL and left that company, which had just set up Cambridge Analytica, in late 2014.[8] Mr. Wylie indicated that he had contacted Jeff Silvester and Zackary Massingham to ask them to work for SCL, and that AggregateIQ (AIQ) had been created to work on SCL projects. He testified that he does not understand why AIQ is denying that it has been created to work on projects for SCL (and later Cambridge Analytica), when the company was established for that specific purpose[9].

He said that, on paper, AIQ is a separately registered company and is wholly Canadian, but that the company operated as if it were a franchise of SCL.[10] Mr. Wylie was also skeptical that AIQ participated in the creation of the Ripon program without having access to the data used in the software, stating: "I don't know how else you can query a database if you don't have access to the database. I do not know how you can perform targeting if you don't have access to the database".[11]

---

7 Ibid.

8 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 May 2018, 0850 (Christopher Wylie, whistleblower).

9 Ibid., 0945 and 0955.

10 Ibid., 0915.

11 Aleksandr Kogan is a professor at Cambridge University in England. He created a Facebook application with a questionnaire asking certain personal questions. The app gave the developers permission to use the profiles of users that downloaded the app, and also all of their "Facebook friends", which is how data was collected from 87 million users globally. The Ripon platform is a software created by AIQ which was used by Cambridge Analytica during the 2016 American presidential election, first for Ted Cruz, and subsequently for Donald Trump. It allegedly used the profiles of American Facebook users collected by Dr. Kogan and sold to Cambridge Analytica.

Mr. Wylie also told the Committee that, during a conversation with Jeff Silvester in the spring of 2017, Mr. Silvester told him that what AIQ had done during the Brexit referendum was "totally illegal."[12] Mr. Silvester denies saying that.[13]

Mr. Wylie stressed that the collection and use of personal data does not always involve nefarious or unethical intent. It is possible to use this information and to distribute key messages without it being detrimental either to these people or to the democratic process (for example, if the targeted messages encourage people to go vote when they would not have done so otherwise). In his opinion, social media is not necessarily a bad thing; it is a tool, and boundaries need to be created to limit how it can be used.[14]

During his testimony, Mr. Wylie suggested several solutions to the Committee:

- It would be beneficial to have Canadian companies that participate in activities relating to political campaigning outside of Canada to register with a regulatory body, as is the case for lobbyists who want to work in a foreign country.[15]

- The government should take a closer look at a company's previous projects before signing a contractual agreement with it (e.g., by verifying whether the company participated in any projects internationally in the last two years that go against Canada's values of promoting democracy).[16]

- There should be better regulations on transparency for targeting, so that messages from companies or political parties that are shared with target audiences are also available to the public.[17]

12 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 May 2018, 0950 (Christopher Wylie).

13 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 April 2018, 0910 (Jeff Silvester, Chief Operating Offier, AggregateIQ).

14 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 May 2018, 1025 (Christopher Wylie).

15 Ibid., 1015.

16 Ibid.

17 Ibid., 1020 and 1025. He suggested, for example, that Facebook and Google could share all the ads that are published on their platforms.

- There should be rules about the legitimate expectations of users involving social media use and their consent regarding data collection by the social media platform.[18]

- Legislators from various countries should work together to find a common solution with respect to issues created by the global nature of the Internet and how countries can make sure that their democracies remain intact.[19]

Damian Collins, Chair of the United Kingdom's Digital Committee, seemed to agree with Mr. Wylie's last suggestion:

> I think co-operation between our committees and by authorities in different countries is so important. These companies and these investigations cross multiple boundaries. To be successful, I think we need to be as integrated as possible…[20]
>
> There obviously will be different countries that have different rules in place, but I certainly think that rules on transparency would be much effective if they could be enforced across the board.[21]

In light of this information, the Committee recommends:

Recommendation 1 on transparency:

That the Government of Canada enact transparency requirements regarding how organizations and political actors, particularly through social media and other online platforms, collect and use data to target political and other advertising based on techniques such as psychographic profiling. Such requirements could include, but are not limited to:

- **The identification of who paid for the ad, including verifying the authenticity of the person running the ad;**

- **The identification of the target audience, and why the target audience received the ad; and**

---

18 Ibid., 1030 and 1035. For example, if Facebook was given access to the contents of a Facebook page in 2008, and facial recognition is now used, is the consent the user granted to provide access to their profile picture still valid?

19 Ibid., 1050.

20 ETHI, *Evidence*, 1st Session, 42nd Parliament, 3 May 2018, 0920 (Damian Collins).

21 Ibid., 1015.

- **Mandatory registration regarding political advertising outside of Canada.**

2. Chris Vickery

Chris Vickery, an expert in data security, explained during his appearance before the Committee on 17 April 2018 that his work focuses on hunting down data breaches:

> Over the last several years, my reputation has grown to be one of a leading authority on the prevalence and causes of data breaches as well as common patterns of incident response by the affected entities. Please note, though, that the data breaches that I locate and secure are not the result of actual computer exploitation or malicious acts. This is just data that has been left out in the open for whatever reason, and nobody realized it until I came along and found it. You may think there probably wouldn't be that much of that, but you'd be surprised. There is quite an epidemic of misconfigurations out on the Internet.[22]

He mentioned he had identified breaches from companies including Verizon, Viacom, Microsoft and Hewlett-Packard, as well as the United States Department of Defense, the Mexican national institute of elections (INE), and Donald Trump's 2016 presidential campaign website.[23]

Regarding AIQ, Mr. Vickery explained that he had learned of its existence on 20 March 2018 by visiting a public website called GitHub where developers collaborate and publish open-source code:[24]

> I saw a reference to @aggregateiq.com in relation to some SCL Group code that was out there and just available to the public. I followed the bread crumbs, figured out what AggregateIQ was, and noticed they had a sub-domain called GitLab. When I viewed gitlab.aggregateiq.com, it occurred to me that the registration was available, and they were in essence inviting the entire world to register for an account on their collaboration portal.
>
> I proceeded to register an account, it let me in, and all of these tools, utilities, credentials, scripts, employee notes and issues, and merge requests were all present before me. I very quickly realized the importance of this and that there would be likely heavy interest from regulators, governments, and the populace of several nations, so I began downloading. Normally, I go to great efforts to protect anybody who may be affected by this type of thing, but the overwhelming public interest in knowing the truth

22 ETHI, *Evidence*, 1st Session, 42nd Parliament, 17 April 2018, 0850 (Chris Vickery, Director of Cyber Risk Research, UpGuard, As an Individual).

23 Ibid.

24 Ibid., 0850 and 0855.

> behind what Cambridge Analytica, AggregateIQ, and SCL Group have been doing is a compelling factor in this particular situation.[25]

According to Mr. Vickery, there are still some unanswered questions. He informed the Committee that, "[w]hile I am still looking into quite a bit of the data, I have not come to the exact final conclusion as to what AggregateIQ's relationship is to SCL Group and Cambridge Analytica. The walls of the separation between those entities are very porous."[26] He believes it is clear that all three entities shared code access permissions and data.[27]

Another matter that the Committee should consider, according to Mr. Vickery, is to what extent AIQ or its employees used private or political data for commercial profit-seeking ventures:

> I have found evidence of ad networks being developed under the same domain, one notably called Ad*Reach network … as well as aq-reach. One of the employees who was working at AIQ was doing simultaneous work for an ad company called easyAd Group AG, which is based in Switzerland and has subsidiaries in the U.S. and in Russia. I would love to know what work was being done and if any of the data travelling through AIQ was utilized in any of those ad campaigns or set-ups that the employee was working on at the same time.[28]

Mr. Vickery also drew the Committee's attention to Midas, a cryptocurrency project that he found online in the AIQ data repository and that involved selling the cryptocurrency for a minimum $10,000 buy-in.[29] According to Mr. Vickery:

> The website has gone down since this was made public, and it feels very fishy to me. If you could figure out why somebody was developing a cryptocurrency on the AggregateIQ GitLab instance, for sale to the public, and why they would possibly not want anyone to know about this, I think it would be worth the investigation.[30]

25 Ibid.

26 Ibid., 0855.

27 Ibid.

28 Ibid.

29 Ibid., 0900.

30 Ibid.

Jeff Silvester, the Chief Operating Officer of AIQ, told the Committee that the cryptocurrency project was a project that AIQ was doing for a client in British Columbia, which has not yet been launched[31].

In response to questions from Committee members, Mr. Vickery explained that, in its documentation, AIQ describes in detail its system for amalgamating various databases. Facebook plays a role in this system, which works as follows:

> It starts with being bootstrapped by the RNC's Data Trust data vault, which is the Republican National Committee here in the United States. I had actually found the Data Trust database before it was part of the find in June 2017. It's quite extensive. It contains data as they merged with i360, which is a Koch brothers-backed political information company. Data Trust deleted a blog entry where they claim to have merged their data with i360.
>
> There's also L2 Political. They provided data to this whole beast of a machine. That was admitted to on Cambridge Analytica's website recently.
>
> Facebook is obviously part of it. The documentation by AggregateIQ goes on to explain that commercial databases are involved. I know that Experian is one that contributed data toward the RNC Deep Root Analytics data briefs that I found in 2017. I know that because there were Experian IDs being lined up to each voter ID with all the consumer habits being tied onto everybody.
>
> AggregateIQ also states that candidates can bring in their own sources of volunteer and supporter and donator information. They'll aggregate all that into the main "database of truth", as they call it. State voter files then corroborate what the RNC has on file.
>
> So there's really no end to what they can plug into here.[32]

Mr. Vickery also explained that SCL and AIQ seem to have worked with the same code base, despite the fact that AIQ representatives have said that there is no link between the two companies.[33] In addition, according to what Mr. Vickery discovered, the code base contains a client field that was filled out with "Cambridge Analytica":

> Now, I can't see why SCL Group would be saying that Cambridge Analytica is a client of theirs. They basically own Cambridge Analytica. SCL Group is the mother ship on top of that. The only reasonable explanation to me is that AggregateIQ would have been the

31 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 April 2018, 0905 (Jeff Silvester).

32 Ibid., 0905.

33 Ibid., 0930.

> one putting Cambridge Analytica as the client, then the code being passed to SCL Group, and that just not being changed immediately. There's a little triangle going on there.[34]

Mr. Vickery pointed out that, in recent public statements, Cambridge Analytica gave examples of data it had used, which indicated a potential link with AIQ documentation:

> More recently, I guess they felt pressure to be transparent about where the data came from. They admitted that they got the RNC Data Trust data. The RNC IDs are all over the place in the fields, categories, targeting scripts, and parsers that are present in AggregateIQ's repository as well as in their documentation. So if data [is transferred] directly from one to the other, they are certainly dealing with the same type of data.[35]

To show how money flowed between Cambridge Analytica and AIQ, Mr. Vickery gave the example of the Ripon platform, used in Ted Cruz's presidential campaign in 2016:

> Ted Cruz's campaign believed they were paying Cambridge Analytica for this product, development, or whatever service, but in actuality it was AggregateIQ that was doing the developing, creating the product, and basically being the workhorse on it, while the cheques were going to Cambridge Analytica.[36]

Mr. Vickery explained that he saw AIQ as a division of a larger entity, comparing it to "a development department within a larger corporation."[37] In his opinion, it is likely that the larger corporation is SCL, as their goals and end points align in parallel.[38]

Lastly, regarding Facebook, Mr. Vickery said that Facebook application usage and potential exploitation is a very widespread issue. He discovered that a Facebook app tied to AIQ (AIQ was identified as a scraper for the app) had been classified as a game in Facebook.[39] AIQ was suspended from the Facebook platform, but according to Mr. Vickery, the identifier for the app still exists within the code he has found.[40]

Mr. Vickery appeared a second time before this committee on 7 June 2018 to answer further questions and to provide additional details relating to his discovery of the AIQ repository. The Committee would like to recognize Mr. Vickery's contribution to the

---

34 Ibid., 0910.

35 Ibid. Due to a technical difficulty during the recording of the evidence, the words ''is transferred'' in this citation are inferred by the Committee.

36 Ibid., 0930.

37 Ibid., 1030.

38 Ibid.

39 Ibid., 1005.

40 Ibid.

study and his useful technical analysis, which helped the Committee better understand the implications of the data breach it was studying.

3. Facebook

Kevin Chan, Global Director and Head of Public Policy for Facebook Canada, and Robert Sherman, Deputy Chief Privacy Officer for Facebook, appeared before the Committee on behalf of Facebook. While acknowledging that Facebook still did not have all the facts about Cambridge Analytica, Mr. Chan said that the situation was "a huge breach of trust" to Facebook users.[41]

The Facebook representatives recognized that the company committed the following mistakes:

- Facebook had not invested enough in the security of its platform, and it takes responsibility for that;[42]
- Facebook did not do enough to prevent these powerful tools from being used for harm;[43]
- Facebook did not take a broad enough view of its responsibility;[44]
- "We recognize that, in the past, we have been too idealistic about the use of our technologies and we have not concentrated sufficiently on preventing abuse on our platform."[45]
- Facebook should have notified users affected by the Cambridge Analytica affair in 2016;[46]

41 ETHI, *Evidence*, 1st Session, 42nd Parliament, 19 April 2018, 0850 (Kevin Chan).

42 Ibid.

43 Ibid.

44 Ibid.

45 Ibid., 0855.

46 Ibid., 0900 (Robert Sherman).

- Regarding the way Facebook's platform worked before changes were made in 2014 to limit the information app developers could collect: "we don't think that's the right way for a platform to operate";[47]

- Facebook was too slow to identify the threat of foreign interference through fake accounts and misinformation during the most recent presidential election in the United States.[48]

The acknowledgment by Facebook that private messages may have been shared without users' consent is of particular concern to the Committee given the high expectation of privacy in such communication[49].

The Facebook representatives said that the company had already taken – or intended to take – the following steps to address the issues that have been identified:

- The week before its representatives appeared before the Committee, Facebook started showing its users the list of the apps they had used and also giving them an easy way to revoke the permissions they had granted to those apps in the past (users could already do this from their privacy settings, but this reminder ensured all users would see it);[50]

- The Communications Security Establishment of Canada's 2017 report identified two areas where Facebook had a role to play: cybersecurity and hacking into the online accounts of candidates and political parties, and also the spreading of misinformation online. In response, Facebook launched its five-point "Canadian election integrity initiative" in the fall of 2017:

    - A "Cyber Hygiene Guide" for Canadian politicians and political parties;

    - Cyber-hygiene training for all federal political parties;

    - A cyber-threats email line for Canadian federal politicians and political parties;

47 Ibid.

48 Ibid., 1005 (Kevin Chan).

49 Ibid., 1035 (Robert Sherman).

50 Ibid., 0850.

  - A partnership with MediaSmarts, Canada's Centre for Digital and Media Literacy, to fight misinformation online; and

  - An "ads transparency test" called "View Ads," which was launched in Canada in November 2017 and allows Canadian Facebook users to view all ads that appear on Facebook, including those for which the user was not the intended audience.[51]

- Facebook is in the process of informing Facebook users in Canada – and elsewhere in the world – if they were affected by the Cambridge Analytica affair by displaying messages at the top of their news feeds that explain that users will have access to information about which apps have collected their personal information;[52]

- Regarding app developers associated with Facebook and other third parties with whom Facebook does business (such as Aleksandr Kogan, for example), Facebook must "invest very heavily in additional personnel and processes to make sure we have oversight in those areas";[53]

- Facebook, and society in general, should invest in more ways of communicating with people about privacy;[54]

- The recent controls announced by Facebook will make it easier for users to control their experience and privacy on Facebook from one central map; before, users may have had to go through 20 different screens to do so;[55]

- Facebook has put in place artificial intelligence tools that help identify fake accounts so they can be taken down before they can be used for nefarious purposes, such as interfering in elections;[56]

51 Ibid., 0855 (Kevin Chan).

52 Ibid., 0900 (Robert Sherman).

53 Ibid., 0945.

54 Ibid., 0950.

55 Ibid., 0855 (Kevin Chan).

56 Ibid., 1010.

- With respect to political ads for the upcoming United States mid-term elections, Facebook will take additional measures to ensure the authenticity of the person running the ad accounts;[57]

- Regarding the issue of large-scale collecting of public information generally available on the Internet, known as "scraping," which Facebook – and any Internet service – must deal with, Facebook has put technical measures in place to address this issue and to identify when it happens.[58]

Mr. Sherman pointed out that Facebook has placed a number of restrictions on the way in which application developers can use the information from a platform, for example:

> [T]hey can't ask for information they don't need to operate their apps. They can't sell information they receive. They can't use it for monetization or app networks or those kinds of things. They have to delete the information if we or somebody else asks them to do so.[59]

Regarding the European Union's implementation of the *General Data Protection Regulation* (GDPR) and its enforcement, Mr. Sherman answered the Committee's questions as follows:

> As a part of our work to prepare for GDPR, we've built a number of new privacy controls settings and other engagements, and those are things that we plan to roll out in Canada as well.[60]

Lastly, Facebook officials agreed to follow up with the Committee and provide a list of all types of personal information that may have been shared without users' consent and the results of the reconciliation between the number of applications that improperly shared information and the number of users affected.[61] At the time of publication of this report, Facebook has yet to provide the committee with this data.

The Committee will ensure that Facebook follows up and it hopes that, once Facebook has completed its internal investigation concerning Cambridge Analytica and all the facts are known, it will respond in a manner commensurate with the problem that has been brought to light.

---

57 Ibid., 1030.

58 Ibid., 1040 (Robert Sherman).

59 Ibid., 1025.

60 Ibid., 0915.

61 Ibid., 1040.

4. AggregateIQ

Given the information it had received, especially from Mr. Vickery, the Committee sought to better understand AIQ's role in the data breach involving Facebook and Cambridge Analytica. Zackary Massingham, Chief Executive Officer, and Jeff Silvester, Chief Operating Officer, appeared on behalf of AIQ on 24 April 2018. Mr. Massingham stated that AIQ is not and never has been a department or subsidiary of SCL or Cambridge Analytica, and that it is wholly Canadian-owned and operated.[62] He also told the Committee that all of the work AIQ does for one client is kept separate from the work done for other clients. In addition, the only personal information that AIQ uses is the information a client provides for specific purposes.[63] According to Mr. Massingham, AIQ has "never managed, had access to or used any Facebook data allegedly improperly obtained by Cambridge Analytica or by anyone else."[64]

Mr. Silvester went on to explain AIQ's work:

> We are not a big data company. We are not a data analytics company. We do not harvest, or otherwise illegally obtain, data. We never share information from one client to another, and we are not a practitioner of the so-called digital dark arts. As Zack said, we do online advertising, make websites, and software for our clients.[65]

He also stated that Facebook and Google provide his company with all the information needed to target a specific audience:

> With Facebook in particular, you can target based on geography, down to a postal code level. You can target an ad based on the general demographic characteristics—male, female, general age category. You can also target based on an interest category. That information is really all you need to create an advertising campaign, and that's provided to us by the client.[66]

Mr. Silvester explained that the presence of personal information in AIQ's code repository was a mistake on the company's part: "It was not supposed to be there. As the person ultimately responsible for that, I'm sorry."[67]

---

62 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 April 2018, 0845 (Zackary Massingham, Chief Executive Officer, AggregateIQ).

63 Ibid.

64 Ibid.

65 Ibid., 0845 (Jeff Silvester).

66 Ibid., 0955.

67 Ibid., 0845.

The Committee does not concur with AIQ's version of the facts, as the witnesses' testimony is inconsistent, full of contradictions, and conflicts with the testimony of several other reliable witnesses. For example, Mr. Massingham stated that AIQ has no connection with SCL, yet he is listed on certain documents as the head of SCL Canada, and SCL listed his direct telephone line as the number for SCL Canada.[68] Mr. Massingham said he was unaware of the reference to his direct line on SCL's website until it was reported in the media.[69] Both Mr. Massingham and Mr. Silvester deny that AIQ ever presented itself as SCL Canada, or that SCL Canada – as an entity – has ever existed[70].

Regarding AIQ's work on Brexit, the campaign to withdraw the United Kingdom from the European Union, Mr. Silvester stated that he was not aware of any coordination among AIQ's four clients involved in the campaign (DUP, BeLeave, Vote Leave and Veterans for Britain).[71]

Mr. Massingham stated further that he did not know there was a BeLeave drive within a Vote Leave drive.[72] Mr. Silvester subsequently corrected Mr. Massingham:

> If I could clarify, we did have access to the Vote Leave drive.…The drive itself was a Vote Leave drive, and images were on that drive. We have access to things like that, that we might use for advertising. Appreciate we did not have access to the entire drive. [73]

Moreover, AIQ received £625,000 pounds (about C$1.1 million) from the Vote Leave campaign to do work on behalf of BeLeave, even though AIQ representatives stated that there was no coordination among the clients campaigning in favour of Brexit. When asked if he was aware that Vote Leave would have violated Britain's election finance law if it had spent this amount in its own name, Mr. Massingham replied, "Yes, that would have put them over their cap."[74]

Mr. Silvester stated that AIQ has been working with the United Kingdom's Information Commissioner since first approached by her office:

---

68 Ibid., 1010 (Zackary Massingham).

69 Ibid.

70 Ibid., 0905, 0910, 1005 and 1010 (Zackary Massingham); Ibid., 0910, 0930, 1010 and 1035 (Jeff Silvester).

71 Ibid., 0855 (Jeff Silvester).

72 Ibid., 0855 (Zackary Massingham).

73 Ibid., 0855 (Jeff Silvester).

74 Ibid., 1015 (Zackary Massingham).

> On May 17, 2017, the Information Commissioner from the U.K. sent us a letter. We responded on May 24, and then we didn't hear from her again until January 30, 2018, when she sent us a letter and we replied.[75]

During AIQ representatives' appearance before the Committee on 24 April, a Committee member received a message from Damian Collins, Chair of the U.K. Digital Committee, which is studying the same issue. Mr. Collins had just spoken with Elizabeth Denham, the U.K. Information Commissioner. She told Mr. Collins that AIQ had refused to answer her specific questions about data usage during the referendum campaign, and that she was considering further legal measures to obtain the information she needed.[76]

AIQ provided the Committee with copies of the two letters it had sent to the U.K. Information Commissioner on 24 May 2017 and 5 March 2018. In the second letter, AIQ representatives stated the following:

> We are not subject to the jurisdiction of your office […]. We consider our involvement in your office's investigation to be closed.[77]

Although, technically, AIQ did respond to the Information Commissioner in the form of two letters, it appears that the Commissioner considered that its replies constituted a refusal to cooperate with her.

During her testimony before the Committee, Ms. Denham reported the lack of co-operation from AIQ, noting however that there has been new communications between the two parties recently which could lead to better collaboration in the future. [78]

The Committee wishes to emphasize that it has complete confidence in Ms. Denham and trusts her judgement. The Committee also notes that Mr. Silvester appeared before the Committee a second time on 12 June 2018 to answer further questions. In general, he made the same statements he had made during his first appearance.

---

75 Ibid., 0855 (Jeff Silvester).

76 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 April 2018, 1010 (Nathaniel Erskine-Smith).

77 Letter from AIQ to the U.K. Information Commissioner's Office, dated 5 March 2018.

78 ETHI, *Evidence*, 1st Session, 42nd Parliament, 24 April 2018, 1010, 1020 and 1025; ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 May 2018, 0905 (Elizabeth Denham, Information Commissioner, United Kingdom Information Commissioner's Office).

PART 2: THE POINT OF VIEW OF ORGANIZATIONS' REPRESENTATIVES

A. Mozilla Corporation

Marshall Erwin, Director of Trust and Security at Mozilla Corporation, appeared before the Committee on behalf of his company. He explained that Firefox, the Mozilla browser, is operated based on a set of data privacy principles that guide Mozilla's data collection practices.[79] As he told the Committee, Mozilla made the decision not to collect data about its users, such as their browsing history; however, it does collect certain information:

> Mozilla does collect a limited set of information from the browser by default to help us understand essentially how people are using the technology. This is information, for example, about the types of features you use in the browser, but it is not about your web-browsing activity itself, which is an important distinction that we make. [80]

Mr. Erwin identified three problem areas regarding the privacy measures that the technology industry takes:

> First, those privacy controls are often buried and difficult to find. The industry does not proactively help people understand and use their privacy settings. As a result, Internet users might have technical privacy controls, but they do not have meaningful control over their privacy today.
>
> Second, the default state of those controls is not reasonable and does not align with users' expectations of what will happen when they use a product or a service. Users are defaulted into the collection and sharing of sensitive data. This violates what we call the sensible settings principle that we practise within Firefox. These sensible settings do not exist for much of the technology industry today.
>
> Third, the data collection and sharing that are tied to those privacy settings are still expansive and permissive. The basic limited data principle—again, one that we practise within Mozilla—is not one that is followed by the industry. [81]

Mr. Erwin stated that these three issues are at play in the case of Facebook and Cambridge Analytica.[82]

---

79 ETHI, *Evidence*, 1st Session, 42nd Parliament, 26 April 2018, 0955 (Marshall Erwin, Director, Trust and Security, Mozilla Corporation).

80 Ibid.

81 Ibid.

82 Ibid.

Mr. Erwin noted that Mozilla decided to pause its advertising on Facebook when the story broke about Cambridge Analytica, and that it has not resumed.[83] This decision was based on the default settings provided to third-party developers. According to Mr. Erwin, these settings were not accurate and seemed to provide data to those developers.[84]

He also touched on Facebook's tracking activities:

> Facebook argued before the U.S. Congress two weeks ago that its cross-site tracking activity is no different than what companies like Twitter, Pinterest, and Google do every day. Facebook was right about that. This is a common tactic across the industry and is not unique to Facebook in any way. [85]

Mr. Erwin made the following recommendation regarding PIPEDA:

> In Canada, if this committee really wants to make an impact here, it would be in that enforcement piece. Again, I think PIPEDA provides a good framework that you might want to make some changes to, but then really strengthening the enforcement part is … useful.[86]

Lastly, Mr. Erwin commented on the European Union's GDPR and its coming into force:

> There is a lot of unease about the GDPR. The bottom line is that companies are very concerned about the levy of a 4% fine, which is baked into the GDPR. Some of that concern is probably healthy and is going to force companies to get to a better place. The challenge with respect to GDPR that I think a lot of companies are facing is just a lack of clarity right now and unease in terms of what companies should really be doing to comply so that they're not going to be subject to those fines. The actual motivating premise of that fine is healthy, and it's useful for the industry to have that. [87]

The Committee notes that Mr. Erwin's recommendation to strengthen the enforcement of PIPEDA and his assessment of the impact of the GDPR on business – two aspects that are interrelated – echo the recommendations made by the Committee in its review of PIPEDA released in February 2018 and reiterated in the present report.

---

83 Ibid.

84 Ibid., 1025.

85 Ibid., 1000.

86 Ibid., 1020.

87 Ibid., 1025.

B. Google

Colin McKay, Head of Public Policy and Government Relations, appeared before the Committee on behalf of Google Canada. He explained the various tools Google offers to protect users' data, such as My Account, Security Checkup, Privacy Checkup, Google Takeout and Google Play Protect.[88]

In response to the Committee's questions and with regard to Mr. Balsillie's recommendation to develop a national data strategy (explained in the next part of the present report), Mr. McKay made his own recommendation:

> The government certainly has an opportunity to create a nuanced strategy that helps Canada differentiate itself from the rest of the world, not just in the tech sector but in health, where we already have quite a lead in terms of dealing with health information, as well as agriculture, mining, and manufacturing.
>
> A data strategy does not need to be as restrictive or prescriptive as Mr. Balsillie has suggested. In fact, a strategy that tries to box Canada in or creates obligations that are not either parallel or similar to those available elsewhere in the world will actually limit the opportunities available to Canadians to innovate, both in Canada and internationally. There needs to be consistency and predictability in any regulatory framework that's set up. [89]

He also emphasized that Google does not sell the personal information of its users, nor does it exchange this information with advertisers.[90]

Mr. McKay made the following comment on the GDPR's coming into force:

> We've been investing in the teams and improving our tools to comply with GDPR for a very long time. It's a tremendously complex challenge, even for a company of our size. It's an even greater challenge, not just for smaller companies, but for the privacy commissioners in Europe, themselves.
>
> What we're doing is reflected in the tools I mentioned in my opening remarks. It's reflected in the sorts of permissions and control that individual users have across all of our services around the world.

---

88 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 May 2018, 0955 (Colin McKay, Head, Public Policy and Government Relations, Google Canada).

89 Ibid., 1010.

90 Ibid.

> You are seeing the echoes of the obligations of GDPR, and the expectations around data protection in Europe, through the services that are provided by Google to users around the world. [91]

The Committee recognizes the impact that the GDPR's coming into force will have on a company of Google's scale.

C. Council of Canadian Innovators

Jim Balsillie, Chair of the Council of Canadian Innovators, appeared on behalf of this organization. In his view, data governance is the most important public policy issue of our time.[92] He explained that the Council of Canadian Innovators called on government to develop a national data strategy "to ensure that cross-border data and information flows serve the interests of Canada's economy":[93]

> A national data strategy should codify explicit treatment of competition in the data sections of free trade agreements, including the right to competitive access to data flowing through large data platforms that have de facto utility status. If Canada doesn't create adequate data residency, localization, and routing laws that protect Canadians, then our data is subject to foreign laws, making Canada a client state.[94]

Mr. Balsillie stated that a national data strategy should also consider competition behaviour and data ownership.[95]

Mr. Balsillie made the following comment on the situation involving Facebook and Cambridge Analytica:

> The Cambridge Analytica and Facebook scandal is not a privacy breach, nor is it a corporate governance issue. It's not even a trust issue. It's a business model issue based on exploiting current gaps in Canada data governance laws.[96]

According to Mr. Balsillie, Facebook and Google are companies built exclusively on the principle of mass surveillance, and that "surveillance capitalism" is the most powerful market force today.[97]

---

91 Ibid., 1045.

92 Ibid., 1000 (Jim Balsillie, Chair, Council of Canadian Innovators).

93 Ibid.

94 Ibid.

95 Ibid., 1045.

96 Ibid., 1000.

97 Ibid.

With respect to the coming into force of the GDPR, he made the following recommendation: implement GDPR-like provisions for Canada.[98]

> GDPR offers valuable lessons and a point of departure for Canada's legislators and regulators. It is a universally acknowledged advance in privacy protection and control of data.[99]

In that context, the Committee makes the following recommendation:

Recommendation 2 on implementing measures in Canada that are similar to the *General Data Protection Regulation*:

That the government of Canada immediately begin implementing measures in order to ensure that data protections similar to the *General Data Protection Regulation* are put in place for Canadians, including the recommendations contained in the report on the *Personal Information Protection and Electronic Documents Act* tabled in February 2018.

As for the law applicable to data, which is constantly moving, Mr. Balsillie provided the following explanation:

> a very central part of the GDPR and this was a tremendous tug-of-war between Brussels and Washington over many years, is this element of safe harbour in routing. It is important to understand that no matter what we regulate in Canada, I've been told by experts that something akin to 80% and 90% of our data is routed through the U.S. Even if I sent you an email across this table, it's routing outside. It's called a boomerang effect. You have to understand that, per U.S. law, Canadian data has no rights whatsoever in the United States. You have no right to privacy; you have no right to anything. What the EU also did was manage the routing so that it never left the jurisdiction of what they prescribed as appropriate treatment of that data.[100]

In this regard, the Committee recommends the following:

Recommendation 3 on data sovereignty:

That the Government of Canada establish rules and guidelines regarding data ownership and data sovereignty with the objective of putting a stop to the non-consented collection and use of citizens' personal information. These rules and guidelines should address the challenges presented by cloud computing.

---

98 Ibid.

99 Ibid.

100 Ibid., 1040.

Lastly, Mr. Balsillie said that privacy and digital services – public and private – are not in conflict, and he referred to Estonia, which "shows that better data governance leads to increased privacy in digital services."[101]

The Committee takes note of Mr. Balsillie's recommendations and will continue studying the example of Estonia as part of its study on the implications on privacy of implementing digital government services in Canada.

PART 3: THE POINTS OF VIEW OF PRIVACY AND INFORMATION COMMISSIONERS AND OF ACADEMICS

A. Current Investigations

The case involving Cambridge Analytica and Facebook and Mr. Wylie's revelations caught the attention of not only the Privacy Commissioner of Canada,[102] but also the Information and Privacy Commissioner for British Columbia[103] and the United Kingdom's Information Commissioner.[104]

1. Privacy Commissioner of Canada

On 20 March 2018, the Office of the Privacy Commissioner of Canada (OPC) issued a news release in which it indicated that it had received a complaint against Facebook regarding alleged unauthorized access and use of Facebook user profiles, and was launching an investigation. The Privacy Commissioner of Canada, Daniel Therrien, has indicated that the investigation will examine Facebook's compliance with Canada's federal private sector privacy law, PIPEDA. He further indicated that the OPC will remain in contact with the U.K. Information Commissioner's Office, which has an ongoing related investigation.[105]

---

101 Ibid., 1000.

102 Office of the Privacy Commissioner of Canada, *Privacy Commissioner launches Facebook investigation*, News Release, 20 March 2018; Office of the Privacy Commissioner of Canada, *BC, federal Privacy Commissioners initiate joint investigations into AggregateIQ, Facebook*, Announcement, 5 April 2018.

103 Office of the Information and Privacy Commissioner for British Columbia, *BC, federal Privacy Commissioners initiate joint investigations into AggregateIQ, Facebook*, News Release, 5 April 2018.

104 United Kingdom, Information Commissioner's Office, "ICO statement: investigation into data analytics for political purposes," 2 May 2018.

105 Office of the Privacy Commissioner of Canada, *Privacy Commissioner launches Facebook investigation*, News Release, 20 March 2018.

On 5 April 2018, the OPC announced that its investigation into Facebook would be conducted jointly with the Office of the Information and Privacy Commissioner for British Columbia (OIPC), which is also conducting an investigation into allegations against AIQ, since the company is located in that province.[106]

2. Office of the Information and Privacy Commissioner for British Columbia

The OIPC launched its investigation into AIQ at the end of 2017.[107] As indicated above, the OIPC and the OPC are conducting joint investigations into AIQ and Facebook. These investigations will examine whether the organizations are in compliance with PIPEDA and British Columbia's *Personal Information Protection Act* (PIPA).[108]

3. United Kingdom's Information Commissioner

The U.K. Information Commissioner is currently conducting an investigation into the use of data and analytics by political campaigns, political parties, social media companies and other commercial actors. She is investigating 30 organizations, including Facebook, and how data were collected from a third-party app on that platform and shared with Cambridge Analytica. Her office is also conducting a broader investigation into how social media platforms are used in political campaigning.[109]

B. Commissioners' Comments about their Enforcement Powers

The Privacy Commissioner of Canada appeared before the Committee on 17 April 2018. Mr. Therrien made the following comments about privacy and his powers under Canadian legislation:

> In Canada, we of course have privacy legislation, but it is quite permissive and gives companies wide latitude to use personal information for their own benefit. Under PIPEDA, organizations have a legal obligation to be accountable, but Canadians cannot rely exclusively on companies to manage their information responsibly. Transparency and accountability are necessary, but they are not sufficient.

106 Office of the Information and Privacy Commissioner for British Columbia, *BC, federal Privacy Commissioners initiate joint investigations into AggregateIQ, Facebook*, News Release, 5 April 2018.

107 Ibid.

108 Office of the Information and Privacy Commissioner for British Columbia, "BC, federal Privacy Commissioners initiate joint investigations into AggregateIQ, Facebook," News release, 5 April 2018.

109 United Kingdom, Information Commissioner's Office, Statement, 2 May 2018.

> To be clear, it is not enough to simply ask companies to live up to their responsibilities. Canadians need stronger privacy laws that will protect them when organizations fail to do so…
>
> Significantly, given the opaqueness of business models and complexity of data flows, the law should allow my office to go into an organization to independently confirm that the principles in our privacy laws are being respected—without necessarily suspecting a violation of the law.
>
> The time has also come to provide my office with the power to make orders and issue financial penalties, helping us to more effectively deal with those who refuse to comply with the law.[110]

Mr. Collins appeared before the Committee on 3 May 2018. He said that one of the reasons his committee supports granting the U.K. Information Commissioner additional powers, including the power to visit certain companies without notice in order to seize information or documents, is that it is difficult to ascertain whether a company is complying with, for instance, the European Union's GDPR:

> I think one of the big questions posed to our inquiry, and why we supported the Information Commissioner's getting these additional powers to support her investigations, is how do we know that a company like Facebook is compliant with GDPR rules? If someone puts in a request to get their data back or to have their data destroyed, how do we know that the request has been complied with? If someone asks for their data back and they want data that's been acquired by Facebook developers, as well, who polices that? The best way we can do that, I think, is to make sure the authorities have got these "no notice" powers just to go in and take data and inspect data where they believe a breach may have occurred.[111]

He added that he believes it is very important for an information commissioner (in the Canadian context, a privacy commissioner) to have not only the authority to order the production of materials, but also the right to seize this information if the company refuses to produce the documents in question, as well as significant fining powers.[112]

On 10 May 2018, the Committee heard from the Information and Privacy Commissioner for British Columbia, Michael McEvoy, and the United Kingdom's Information Commissioner, Elizabeth Denham.

---

110 ETHI, *Evidence*, 1st Session, 42nd Parliament, 17 April 2018, 0845 (Daniel Therrien, Privacy Commissioner of Canada).

111 ETHI, *Evidence*, 1st Session, 42nd Parliament, 3 May 2018, 0930 (Damian Collins).

112 Ibid., 1010.

In British Columbia, PIPEDA is superseded by the PIPA, since the provincial legislation is recognized as being essentially similar to the federal legislation. Under PIPA, that province's information and privacy commissioner has broader enforcement powers than those of the Privacy Commissioner of Canada. For example, he can impose fines and issue orders. Mr. McEvoy explained:

> Our office is on record as supporting Parliament providing greater powers to the Office of the Privacy Commissioner of Canada.
>
> It's really from the perspective of citizens that I think we need to think about this. Given the matters that you're investigating, Canadians want to have some sense that somebody with some regulatory power has their backs. That can't happen unless the regulator has the appropriate authority to ensure that these kinds of things are properly remedied if there is a concern with or a transgression of the law.[113]

The *Data Protection Act 1998* (DPA) also provides Ms. Denham with broader enforcement powers than those of the Privacy Commissioner of Canada. She contrasted these powers with those of her Canadian counterpart:

> […] the Canadian Privacy Commissioner's powers have fallen behind the rest of the world, so having order-making power, having the ability to levy administrative penalties, civil monetary penalties, and certainly the ability to seize material and to act quickly, I think are really important when we're dealing with global data companies and fast-paced investigations.
>
> Even the powers that I have under the current U.K. Data Protection Act were not sufficient in this case. Government has moved really quickly and tabled amendments, which were passed last night, to provide us with even more powers of no notice inspections, streamlined warrants, the ability to make emergency orders, and also criminal sanctions for destruction of records and information.
>
> That's important in the broader context with digital companies and being able to move quickly in the public interest[114].

In light of the preceding and even though the Committee's study is not yet completed, the Committee believes that the recommendations it made in February 2018 about the powers of the Privacy Commissioner of Canada in its report "*Towards Privacy by Design: Review of the* Personal Information Protection And Electronic Documents Act" (PIPEDA

113 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 May 2018, 0910 (Michael McEvoy, Commissioner, Office of the Information and Privacy Commissioner for British Columbia).

114 Ibid., 0910 (Elizabeth Denham).

Report)[115] have become even more important. Given recent developments in the security of citizens' online personal information internationally, these recommendations have even taken on a certain urgency.

The Committee believes that it is imperative that the Commissioner be granted more powers in order to protect the privacy of Canadians. It therefore reiterates the following recommendations from its PIPEDA Report:

Recommendation 4 on the Privacy Commissioner's enforcement powers:

That the *Personal Information Protection and Electronic Documents Act* be amended to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance.[116]

Recommendation 5 on the Privacy Commissioner's audit powers:

That the *Personal Information Protection and Electronic Documents Act* be amended to give the Privacy Commissioner broad audit powers, including the ability to choose which complaints to investigate.[117]

As mentioned above, Ms. Denham said that despite all the powers she has under U.K. legislation, she still faced obstacles in the course of her investigation, such as the requirement to wait several days in order to receive the warrant she wished to obtain in order to seize documents from the offices of Cambridge Analytica:

> […] I agree with you that the current provisions in our law don't allow us to move quickly with a warrant. We need to be able to respond to digital crimes and data crimes. The government has just tabled amendments that are going to give us new powers to be able to react more quickly and not have to give long notice periods to organizations. That said, we have been able to seize and secure a great deal of data from Cambridge Analytica, and we have executed two more warrants in this investigation, so we do have a great deal of information. If there are links between one company and another, and if their intellectual property and their data are being used by a new company, then we are able to investigate and continue our investigation. If a company is entering into

115 ETHI, *Towards Privacy by Design: Review of the* Personal Information Protection And Electronic Documents Act, Twelfth Report, 1st Session, 42nd Parliament, February 2018, Recommendations 15 and 16.

116 This recommendation is the same as Recommendation 15 in: ETHI, *Towards Privacy by Design: Review of the* Personal Information Protection And Electronic Documents Act, Twelfth Report, 1st Session, 42nd Parliament, February 2018, p. 61.

117 This recommendation is the same as Recommendation 16 in: ETHI, *Towards Privacy by Design: Review of the* Personal Information Protection And Electronic Documents Act, Twelfth Report, 1st Session, 42nd Parliament, February 2018, p. 62.

> insolvency, as in this case, then we are in touch with the administrators and we're able to proceed with enforcement action, both criminal and civil.[118]

With regard to the new powers granted to the United Kingdom's Information Commissioner, Mr. Collins stated the following:

> The government has already given ground on one of the issues we have championed, and that is on additional powers for the Information Commissioner, for her to be able to have no notice period before arriving to take and seize data, so we don't have a repeat of what was a farcical situation where it took her five days to get a warrant to go into Cambridge Analytica. She will have substantially enhanced powers, which will help the conclusion of this investigation and future ones too.[119]

The Committee believes that such powers should also be included in an amendment to PIPEDA and, in addition to the powers recommended above, recommends the following:

Recommendation 6 on the Privacy Commissioner's additional enforcement powers:

That the *Personal Information Protection and Electronic Documents Act* be amended to give the Privacy Commissioner additional enforcement powers, including the power to issue urgent notices to organizations to produce relevant documents within a shortened time period, and the power to seize documents in the course of an investigation, without notice.

Lastly, Mr. Therrien said that although he has considerable latitude to cooperate with privacy regulators in other jurisdictions, nothing in the legislation allows him to share information with other regulators, such as the Competition Bureau of Canada. The OPC's investigations surrounding PIPEDA could involve both privacy and competition issues. He believes that the OPC's inability to share information with other regulators is a gap in the legislative framework.[120]

The Committee agrees with Mr. Therrien and recommends:

Recommendation 7 on the sharing of information between the Privacy Commissioner and other regulators:

That the *Personal Information Protection and Electronic Documents A*ct be amended to allow the Privacy Commissioner to share certain relevant information in the context of investigations with the Competition Bureau, other Canadian regulators and regulators at the international level, where appropriate.

---

118 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 May 2018, 0905 (Elizabeth Denham).

119 ETHI, *Evidence*, 1st Session, 42nd Parliament, 3 May 2018, 0900 (Damian Collins).

120 ETHI, *Evidence*, 1st Session, 42nd Parliament, 17 April 2018, 0925 and 0930 (Daniel Therrien).

C. Applying Privacy Legislation to Political activities

The Government of Canada recently tabled Bill C-76, the *Elections Modernization Act*, which amends the *Canada Elections Act*.[121] One of the purposes of the bill is to add privacy provisions. These would require Canada's political parties to adopt and maintain a privacy policy and to post it online.[122]

Under the bill, any party that contravenes the privacy provisions may not be able to become a registered party or could lose the right to be registered. However, the proposed changes do not subject political parties to any privacy legislation.

Mr. Therrien raised the lack of privacy legislation applicable to political parties:

> Another area ripe for action concerns privacy protections and political parties.
>
> As you are aware, no federal privacy law applies to political parties; British Columbia is the only province with legislation that covers them.
>
> This is not the case in many other jurisdictions. The UK, much of the EU and New Zealand all cover political organizations with their laws.
>
> In point of fact, in many EU states, information about political views and membership is considered highly sensitive, even within existing data protection regimes, requiring additional protections.
>
> There are also now – in the digital environment – so many more actors involved: data brokers, analytics firms, social networks, content providers, digital marketers, telecom firms and so forth.
>
> So while I am currently investigating commercial organizations such as Facebook and Aggregate IQ, I am unable to investigate how political parties use the personal information they may receive from corporate actors.
>
> In my view, this is a significant gap.[123]

Mr. Therrien also said that adopting a privacy policy is not enough:

---

121 House of Commons of Canada, Bill C-76, An Act to amend the Canada Elections Act and other Acts and to make certain consequential amendments.

122 Democratic Institutions, Backgrounder, *Empowering political parties to better protect Canadians' privacy*, 30 April 2018.

123 Ibid., 0850.

> The situation currently is that most federal political parties have privacy policies – internal codes of conduct, so to speak, in their relationship with the people with whom they interact and from whom they collect information. That's a start.
>
> I think, first of all, the substance of these policies could be improved, from what we have seen. One common element missing from the privacy policies of federal parties is the right of individual electors to have access to the information that parties have about them. That's a huge flaw. There is, then, the issue of the substance. But these are voluntary codes, and no one independent of the parties examines whether the parties actually live up to the promise they're making in these policies. That leads me to a very important reason that political parties should be governed by legislation: to ensure that whatever substantive rules exist, hopefully better than what they are now, are verified by an independent third party.[124]

He described the grey area that political parties are in:

> On the other hand, when I talked about a grey area, it was in the sense that, since I do not have the jurisdiction to verify how the parties use the information, I do not know what is going on. Parties have privacy policies in place to ensure a minimum of rules in their dealings with voters. However, neither I nor any other independent person can verify what is happening. So that's what I meant by "grey area," an area with no independent arbitrator who can ensure that the rules in place are followed.[125]

On April 26, 2016, the Committee heard from Colin Bennett, Professor with the Department of Political Science at the University of Victoria, and Thierry Giasson, Full Professor with the Department of Political Science at Laval University and Director of the Groupe de recherche en communication politique at that university. They both share the opinion that political parties should be subject to privacy legislation. According to Dr. Bennett,

> My second point is that there is a pressing need to bring our political parties within Canada's regime of privacy protection law. I have testified about this to you before. One of the keys to preventing the kinds of abuses we've seen in other countries is to establish some clearer and consistent rules on the kinds of data that political parties may use for campaigning purposes. We need to establish a level playing field that essentially prevents companies like Cambridge Analytica from engaging in the same practices in Canada that have been witnessed elsewhere.
>
> We are one of the only advanced democratic countries where privacy protection law does not cover political parties. For the most part, they are not covered by PIPEDA. They are not government agencies. They are not covered by the Privacy Act. They are also largely and expressly exempt from the anti-spam legislation, as well as from some of the

124 ETHI, *Evidence*, 1st Session, 42nd Parliament, 17 April 2018, 0915 (Daniel Therrien).

125 Ibid., 0940.

> do-not-call list regulations administered through the CRTC. There are privacy and security rules within the Canada Elections Act, but these apply to the voters lists, not to other sources of personal information.
>
> Thus, with respect to political parties, Canadians do not have the legal rights that they have with respect to both government agencies and commercial operations.[126]

In Dr. Bennett's view, the status quo is clearly untenable, since the use of personal data in elections will only increase leading up to the federal election of 2019, particularly with respect to political micro-targeting on Facebook.[127] Dr. Giasson expressed the same view, saying that despite growing media interest in the use of voter analytics and algorithms in election campaigns, "everything that is going on … is being done without Canadians' knowledge, and most Canadians are largely unaware of the extent and effect of the parties' use of their private data."[128] He believes that this is having an impact on Canadian democracy:

> The core question of the debate we are having right now is that there is no transparency. People are not aware of what parties are doing. The fact that parties are doing targeting is not necessarily a huge issue. As you say, advertising and electoral communication are, and always have been, a targeted business. However, the fact that citizens are not aware of what parties are doing with the data they're collecting is a problem, and that's the core problem. Parties need to ensure that whenever citizens grant access to any form of data that could be used for a political targeting purpose, they must be made aware of that.[129]

Dr. Bennett believes that political parties should comply with the 10 PIPEDA principles. He also recommends adopting a certain degree of consistency with respect to the privacy practices of political parties.[130] He noted the dilemma created by the fact that on the one hand, the Chief Electoral Officer knows political parties and the principles that apply to them, but does not have the expertise or the resources necessary to deal with privacy issues; and on the other hand, the Privacy Commissioner has the skills and resources to deal with privacy issues, but does not have the legislative mandate to do so when these matters involve political parties.[131]

---

126 ETHI, *Evidence*, 1st Session, 42nd Parliament, 26 April 2018, 0845 and 0850 (Colin Bennett, Professor, Department of Political Science, University of Victoria).

127 Ibid., 0850.

128 Ibid., 0905 (Thierry Giasson, Full Professor, Department of Political Science, Université Laval).

129 Ibid., 0910.

130 Ibid., 0920 and 0930 (Colin Bennett).

131 Ibid., 0925.

Mr. McEvoy told the Committee that British Columbia is the only province where political parties have obligations under privacy legislation, where PIPA applies to them. He said the following about the impact of adopting such legislation in his province:

> Political parties in my province have been subject to PIPA since its enactment in 2004. In the 14 years that have since passed, I can assure you that democracy has continued to thrive unimpeded in British Columbia. We have not heard concerns or suggestions that laws protecting the personal information of voters restricts the ability of political parties or candidates to engage voters.
>
> Political parties in B.C. can and do collect personal information about voters, but they do so under the same reasonable legal responsibilities and obligations that apply to other organizations.
>
> Generally, this means political parties get information with the consent of voters accompanied by a clear explanation of how and for what purpose that information will be used…
>
> PIPA also gives citizens the legal right to request and correct the personal information that political parties collect from them and to register a complaint if necessary. These complaints are adjudicated by my office. A citizen's right to exert control over their personal information is a fundamental principle of privacy law. It is a principle strengthened by the EU's general data protection regulation […][132]

Mr. McEvoy also cited a case where the British Columbia information and privacy commissioner's ability to investigate the collection of personal information by political parties proved to be quite useful:

> [I]n British Columbia we have had occasion to investigate instances where, in the governing party's collecting information, there were allegations that it may have crossed a line, a grey zone, where that information moved, potentially or allegedly, from a government collection to party sources.
>
> Without our ability to investigate parties, that investigation would have been stopped at that door, which I think would have been not just problematic in terms of our own investigation, but also in terms of the public understanding of what had truly happened to the information that was collected. Because we have a law that allows us to look at parties, we were able to look at that matter holistically and come to conclusions about what had actually happened to the data. I think that enhanced the public's confidence that data was being handled properly, and where it wasn't, that sanctions were available for our office to bring down.[133]

---

132 ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 May 2018, 0900 (Michael McEvoy).

133 Ibid., 0920.

Mr. McEvoy had the following say about Bill C-76, which amends the *Canada Elections Act*:

> Of Course, I know that recent proposed amendments to the *Canada Elections Act* will require political parties to adopt a policy to protect personal information and to provide it to the Chief Electoral Officer. These proposals are only a minimal step forward. They attempt to address the principle of transparency, but that is only one element of a proper data protection regime.[134]
>
> The proposed amendments do not require parties to respond to a voter's request for the information the party holds about them, nor does it allow a voter the right to ask a party to correct inaccurate information about them. Perhaps most important, there is no provision for an impartial third party to hear and determine a voter complaint. These basic legal standards have been a part of British Columbia law for years and are the norm in many western democracies. There should be nothing for political parties to fear in any of these legal obligations. In fact, implementation will do nothing but enhance the confidence of citizens in their democratic institutions.[135]

Ms. Denham told the Committee that political parties in the United Kingdom are also subject to privacy legislation:

> In the U.K. and across the EU, information about individuals' political opinions is considered a particularly sensitive category of personal data to which additional safeguards under data protection law are applied. What that means, therefore, is that political parties and campaigns are subject to a combination of data protection, direct marketing, and electoral law when engaging in processing of data for electoral purposes with oversight by my office and the electoral commission. This has always been the case since data protection legislation was first introduced more than two decades ago, and it's simply accepted as a cultural norm.
>
> These rules are there to ensure free and fair elections, and they do not undermine democratic engagement in the U.K. Instead, political parties have to engage with voters in a manner consistent with that law. Recognizing the special place of political parties in a democratic society, they've been given special status under U.K. data protection law to allow parties to carry out their campaigning activity.
>
> In my complaint-handling role, I consider complaints from individuals against political parties when they think that their data has been misused. The number of complaints has never been particularly high. Other than a spike at election time, political parties have not, in the main, been a sector generating a high proportion of complaints.
> My office has maintained an ongoing dialogue with parties, meeting with them regularly and issuing bespoke guidance on how they can comply with the law when they are campaigning[136]

134 Ibid., 0900.

135 Ibid., 0905.

136 Ibid., 0845 (Elizabeth Denham).

Mr. Wylie expressed some reservations to the Committee about subjecting political parties to privacy legislation, saying that privacy legislation applicable to political parties should not be too restrictive, as this could have a negative rather than positive impact on democracy. He said that if the rules prevented parties from engaging with certain voters and cut off a part of the electorate from political speech, there may not be the challenging discussions brought about by the democratic process.[137]

In light of what the Committee heard, it believes that Canadians would have greater confidence if they knew that their political parties were not exempt from privacy legislation and that they have legal responsibilities similar to those imposed on public and private organizations under the *Privacy Act* and PIPEDA. Any legislative amendment should obviously take the special activities of political parties into account so as not to entirely prevent the use of personal information, but rather to better regulate its collection and use and the transparency surrounding the management of such information.

Consequently, the Committee recommends:

Recommendation 8 on the application of privacy legislation to political activities:

That the Government of Canada take measures to ensure that privacy legislation applies to political activities in Canada either by amending existing legislation or by enacting new legislation.

CONCLUSION

As remarked by Commissioner Therrien, "[t]he integrity of our democratic processes – as well as trust in our digital economy – are both clearly facing significant risks."[138] His remarks were echoed by other witnesses.[139] The revelations about Cambridge Analytica and Facebook have exposed the risk of the malicious collection of personal information, but the Committee is also aware that other organizations are probably engaging in such activities. The recommendations made by the Committee in this preliminary report are a step toward a better protection of Canadians' privacy.

137 ETHI, *Evidence*, 1st Session, 42nd Parliament, 29 May 2018, 1055 (Christopher Wylie)

138 ETHI, *Evidence*, 1st Session, 42nd Parliament, 17 April 2018, 0850 (Daniel Therrien).

139 Ibid. (Chris Vickery); ETHI, *Evidence*, 1st Session, 42nd Parliament, 26 April 2018, 1000 (Marshall Erwin); ETHI, *Evidence*, 1st Session, 42nd Parliament, 10 May 2018, 1005 (Jim Balsillie).

While PIPEDA currently enjoys adequacy status under the GDPR, the Committee urges the government of Canada to implement the various recommendations it made in the PIPEDA report as well as the preliminary recommendations contained in the present report. These recommendations would enhance privacy protection in Canada and make Canadian legislation more closely aligned with the GDPR. The urgency of the matter cannot be overstated.

The Committee intends to continue its study and its cooperation with parliamentarians and regulators in the United Kingdom and the United States in order to determine the range of available means to mitigate the risks that our democratic processes and digital economy are facing. The Committee will make additional recommendations in its final report once its study is completed.

APPENDIX A
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
As an individual Chris Vickery, Director of Cyber Risk Research UpGuard	2018/04/17	99
Office of the Privacy Commissioner of Canada Daniel Therrien, Privacy Commissioner of Canada Barbara Bucknell, Director Policy, Parliamentary Affairs and Research		
Facebook Inc. Kevin Chan, Global Directeur and Head of Public Policy Facebook Canada Robert Sherman, Deputy Chief Privacy Officer	2018/04/19	100
AggregateIQ Zackary Massingham, Chief Executive Officer Jeff Silvester, Chief Operating Officer	2018/04/24	101
As an individuals Colin J. Bennett, Professor Department of Political Science, University of Victoria Thierry Giasson, Full Professor Department of Political Science, Université Laval	2018/04/26	102
Mozilla Corporation Marshall Erwin, Director Trust and Security		
United Kingdom House of Commons Digital, Culture, Media and Sport Select Committee Damian Collins, Chair, MP	2018/05/03	104
Council of Canadian Innovators Jim Balsillie, Chair	2018/05/10	106
Google Canada Colin McKay, Head, Public Policy and Government Relations		

Organizations and Individuals	Date	Meeting
Office of the Information and Privacy Commissioner for British Columbia Michael McEvoy, Commissioner		
United Kingdom Information Commissioner's Office Elizabeth Denham, Information Commissioner		
House of Commons André Gagnon, Deputy Clerk, Procedure House of Commons Wendy Gordon, Director, Legislation Services Office of the Law Clerk and Parliamentary Counsel Stéphane am Rhyn, Legal Counsel Office of the Law Clerk and Parliamentary Counsel	2018/05/24	108
As an individual Christopher Wylie	2018/05/29	109
Office of the Privacy Commissioner of Canada Daniel Therrien, Privacy Commissioner of Canada Barbara Bucknell, Director Policy, Parliamentary Affairs and Research Brent Homan, Executive Director Personal Information Protection and Electronic Documents Act Compliance Directorate Sarah Speevak, Legal Counsel	2018/05/31	110
As an individual Chris Vickery	2018/06/07	112
AggregateIQ Jeff Silvester, Chief Operating Officer	2018/06/12	113

APPENDIX B
LIST OF BRIEFS

Organizations and Individuals

Eatz, Sydney

MINUTES OF PROCEEDINGS

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 99, 100 to 102, 104, 106, 108 to 114) is tabled.

Respectfully submitted,

Bob Zimmer
Chair

Dissenting Report of the New Democratic and Conservative Parties
Breach of Personal Information Involving Cambridge Analytica and Facebook

I. Introduction

In the course of the Committee on Access to Information, Privacy and Ethics' study on the breach of personal information involving Cambridge Analytica and Facebook, the Committee heard from Jeff Silvester and Zack Massingham of AggregateIQ (AIQ), a political consulting firm based in Victoria, B.C.

It was the unanimous view of the Committee that this testimony was contradicted by evidence presented by other witnesses.

Mr. Massingham appeared to be reticent to answer in a fulsome manner during his initial appearance before the Committee, which prompted the Committee to issue a summons to appear again.

Mr. Massingham failed to appear again when summoned, which has raised serious questions about the ability of parliamentary committees to conduct their work unobstructed on behalf of Parliament and the people of Canada.

II. Background

In the gathering of evidence and testimony as part of this study, disturbing allegations were raised about the role of AIQ in democratic processes around the world. Testimony from witnesses directly contradicted statements that were made by Mr. Silvester and Mr. Massingham to our committee.

It is not the role of the committee to find fault with individuals, but to provide Parliament with a clear picture of the facts with possible recommendations for legislative changes. To this end, a summons was issued to Mr. Massingham to give him the opportunity to clarify their original testimony and to respond to the evidence from other witnesses.

In correspondence with Mr. Massingham's counsel about a possible appearance before the Committee on June 12, 2018, the Committee was given evidence that he was unable to appear.

The Committee unanimously decided that the evidence presented to us was not sufficient to rescind the summons for June 12, and we expected his appearance on that day.

On June 12, Mr. Massingham failed to appear before the Committee. No explanation was sent.

III. Conclusion and Recommendations

The New Democratic and Conservative members of the Committee believe that Mr. Massingham's failure to respond to the Committee's summons is an impediment to the Committee's ability to find fact and report our findings to the House of Commons.

In the opinion of the New Democratic and Conservative members of the Committee, allowing Mr. Massingham's actions to stand unchallenged would set a lasting precedent that could undermine the ability of other Members of Parliament and Committees to gather witness testimony from witnesses on issues of national importance.

We believe that the Committee and its Chair have acted appropriately throughout this process towards Mr. Massingham and we have attempted to ensure that the Committee respect its mandate and limits. However, the issue of a witness who refuses a summons from committee requires guidance from the House of Commons.

Questions of privilege must be raised as soon as practicably possible after they arise to be in order before the House. The New Democratic and Conservative members feel strongly that it this refusal to respond to a summons by committee represents a *prima facie* breach of privilege of parliamentarians and a possible ruling of contempt against the House.

The members therefore recommend that the Chair of the Committee be directed to raise the breach with the House of Commons as soon as possible for the consideration of the Speaker.