HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

DEMOCRACY UNDER THREAT: RISKS AND SOLUTIONS IN THE ERA OF DISINFORMATION AND DATA MONOPOLY

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

Bob Zimmer, Chair

DECEMBER 2018
42nd PARLIAMENT, 1st SESSION

DEMOCRACY UNDER THREAT: RISKS AND SOLUTIONS IN THE ERA OF DISINFORMATION AND DATA MONOPOLY

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

Bob Zimmer
Chair

DECEMBER 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 (Parliamentary Secretary — Non-Voting Member)
Michel Picard
Raj Saini
Anita Vandenbeld

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Ziad Aboultaif
Hon. Maxime Bernier
Alexandre Boulerice
Hon. Tony Clement
Don Davies
Kerry Diotte
Andy Fillmore
Greg Fergus
Iqra Khalid
Bernadette Jordan (Parliamentary Secretary — Non-Voting Member)
Michael Levitt
Wayne Long

Alistair MacGregor
Kelly McCauley
Irene Mathyssen
Brian Masse
Eva Nassif
Jean-Claude Poissant
Don Rusnak
Francis Scarpaleggia
Terry Sheehan
Marwan Tabbara
Dave Van Kesteren
Mark Warawa

CLERK OF THE COMMITTEE

Michael MacPherson

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

SEVENTEENTH REPORT

Pursuant to its mandate under Standing Order 108(2), 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 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the committee) began a study of the breach of personal information involving Cambridge Analytica and Facebook. The scandal quickly brought to light much broader questions relating to the self-regulation of platform monopolies, the use of these platforms for data harvesting purposes, and their role in the spreading of disinformation and misinformation around the world.

In June 2018, the committee published an interim report, noting its concern that the Canadian democratic and electoral process is vulnerable to improper acquisition and manipulation of personal data. It made eight preliminary recommendations with respect to the powers of the Privacy Commissioner of Canada, the application of privacy legislation to political activities, requirements regarding transparency in political advertisements, data sovereignty, and the need to better align federal privacy legislation with the European Union *General Data Protection Regulation* (GDPR).

The committee pursued its study this fall. It heard evidence on a variety of topics, including the structural problems inherent to social media platforms, the interaction between privacy law and competition law in the context of data monopolies, cybersecurity, and digital literacy.

After hearing additional evidence, the committee remains of the view that the Government of Canada must act urgently to better protect the privacy of Canadians. To that end, in addition to the preliminary recommendations put forward in June 2018, the committee is of the view that the Government of Canada should:

- subject political parties and political third parties to the *Personal Information Protection and Electronic Documents Act* (PIPEDA);
- provide additional resources to the Office of the Privacy Commissioner to ensure efficient exercise of its additional powers;
- ensure that no foreign funding has an impact on elections in Canada;
- ensure transparency in online political advertisements;
- impose certain obligations on social media platforms regarding the labelling of content produced algorithmically, the labelling of paid advertisement online, the

removal of inauthentic and fraudulent accounts, and the removal of manifestly illegal contents such as hate speech;

- provide to an existing or a new regulatory body the mandate to proactively audit algorithms;
- include principles of data portability and interoperability in PIPEDA;
- study the potential economic harms caused by data-opolies and determine whether the *Competition* Act should be modernized;
- study how cyber threats affect democratic institutions and the electoral system;
- conduct research regarding the impacts of online disinformation and misinformation as well as the cognitive impacts of digital products which create user dependence; and
- invest in digital literacy initiatives.

As stated in its preliminary report, the committee is hopeful that this work will contribute to a lasting solution for a global challenge.

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.

INTRODUCTION

On 17 April 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) began its study on the breach of personal information involving Cambridge Analytica and Facebook (the breach). The Committee quickly learned that the breach was only the tip of the iceberg and that it raised a myriad of important questions.

On 19 June 2018, the Committee presented an interim report to the House of Commons entitled *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process* to detail the Committee's work to that point and to make a number of preliminary recommendations.

Between 25 September and 1 November 2018, the Committee continued its study in order to further explore certain topics and to study other issues that arose during its first series of hearings. The additional evidence gathered has enabled the Committee to present its final report.

In all, the Committee devoted 18 public meetings to this study, during which it heard from 47 witnesses, some of them having testified more than once. It also received two briefs.

CHAPTER 1: AN UNEXPECTED STUDY

Like millions of Canadians, the Committee was surprised when the breach was reported in March 2018. Even though questions about the personal data collection practices of social media platforms had been raised before, the breach – which reportedly provided access to the profiles of approximately 87 million Facebook users – sent shockwaves around the world. The breach elicited impassioned responses from many academics, journalists and citizens, led to investigations and attracted the interest of parliamentary committees in Canada and elsewhere.

The Committee initially focused on the breach and the possibility that Canadians had been affected. It heard testimony from the parties involved: Facebook, AggregateIQ (AIQ), Christopher Wylie and Chris Vickery, a cybersecurity expert who discovered an online database belonging to AIQ. The Committee also invited some of the commissioners conducting investigations into the breach to appear: the Privacy Commissioner of Canada , the Information and Privacy Commissioner for British Columbia and the United Kingdom (U.K.) Information Commissioner.

In addition, the Committee heard from the Chair of the U.K. Digital, Culture, Media and Sport Committee (the "U.K. Committee"), Damian Collins, whose committee is studying disinformation. The U.K. Committee took a particular interest in AIQ, a Canadian business that played a role in the Brexit referendum. The Committee sought to clarify the situation concerning AIQ. The work of the Committee and its findings on AIQ are set out in Chapter 2 of this report.

Finally, the Committee heard from experts, academics, other platforms and technology industry stakeholders. Their testimony enriched the discussion, identified potential solutions and raised further questions, which are addressed in this report. The evidence the Committee heard between April and June 2018 enabled it to make eight preliminary recommendations.[1]

Building on the preliminary recommendations and making use of the new evidence it heard, the Committee reiterates its recommendations of June 2018 and makes new ones to mitigate the threat to democracy in the era of disinformation and data monopolies. The Committee hopes that the results of its work will enable the federal government to better understand the issues Canada is facing and encourage it to take action.

1 The preliminary recommendations are included in the present final report and listed at the end of Chapter 8 as recommendations 19 to 26.

CHAPTER 2: AGGREGATEIQ

FURTHER TESTIMONY FROM ZACKARY MASSINGHAM

On 27 September 2018, Zackary Massingham, Chief Executive Officer of AIQ, appeared before the Committee. He had previously appeared on 24 April 2018 alongside Jeff Silvester, Chief Operating Officer of AIQ. Mr. Silvester appeared again, alone, on 12 June 2018. During his appearance on 27 September, Mr. Massingham made essentially the same statements as he and Mr. Silvester had made during their previous appearances.

In summary, they stated that AIQ had no relationship with Cambridge Analytica or SCL Group (SCL), that they had never seen evidence that the organizations Vote Leave and BeLeave coordinated on the Brexit campaign, and that they were unaware that the personal information provided by SCL had been illegally obtained from Facebook.

The Committee believes that the AIQ representatives, both individually and collectively, did not provide satisfactory answers to its questions and that the evidence heard remains problematic in many respects.

In the interim report it presented in June 2018, the Committee noted that it did not concur with the version of the facts presented by the AIQ representatives at that point because their testimony was inconsistent, full of contradictions and contrary to the testimony of several other reliable witnesses.[2] The Committee also observed that AIQ representatives had failed, during a certain period, to cooperate with the investigation of the U.K. Information Commissioner, Elizabeth Denham.[3]

INVESTIGATIONS BY OVERSIGHT AND MONITORING BODIES

Investigation of the United Kingdom Electoral Commission

On 17 July 2018, the U.K. Electoral Commission, an independent organization that supervises elections and referenda and oversees political funding, published an investigation report on the spending and funding of the Brexit referendum campaign in

2 House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI], *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, p.17.

3 Ibid., p. 18.

2016.[4] While the Electoral Commission's investigation did not directly concern AIQ or its representatives, the firm was at the heart of the investigation, which mainly concerned five payments made to AIQ in June 2016.[5]

Regarding the connection between the spending of Darren Grimes, BeLeave and Vote Leave, which the investigation directly addressed, the Electoral Commission reached the following conclusion:

> The Commission is satisfied beyond reasonable doubt that all Mr Grimes' and BeLeave's spending on referendum campaigning was incurred under a common plan with Vote Leave. This spending, including the £675,315.18 for services from Aggregate IQ reported by Mr Grimes, should have been treated as incurred by Vote Leave.[6]

The fact that the spending of Mr. Grimes and of BeLeave was coordinated with that of Vote Leave led the Electoral Commission to conclude that Vote Leave had exceeded the statutory referendum spending limit.[7]

Furthermore, the report of the Electoral Commission stated that Veterans for Britain inaccurately and illegally reported having received and accepted a cash donation of £100,000 on 20 May 2016, when it was in fact a direct payment made by Vote Leave to AIQ on 29 June 2016 for services provided to Veterans for Britain during the final days of the Brexit referendum campaign.[8]

The Electoral Commission wrote that, while Vote Leave and Veterans for Britain officials knew each other and had worked together, and Vote Leave had recommended the services of AIQ to Veterans for Britain, "The evidence we have seen does not support the concern that the services were provided to Veterans for Britain as joint working with Vote Leave."[9]

Moreover, the Electoral Commission drew the following conclusion regarding the coordination between the parties involved and the handling of data by AIQ:

---

4 United Kingdom [U.K.], The Electoral Commission, *Report of an investigation in respect of - Vote Leave Limited - Mr Darren Grimes - BeLeave - Veterans for Britain Concerning campaign funding and spending for the 2016 referendum on the UK's membership of the EU*, 17 July 2018.

5 Ibid., para. 1.12, p. 5.

6 Ibid., para. 1.14, and para. 4.1, p. 16.

7 Ibid., para. 1.16, p. 6, and para. 4.25, p. 21.

8 Ibid., para. 1.23, p. 7, and para. 4.63, p. 28.

9 Ibid., para. 1.24. See also Ibid., para. 4.69, p. 29.

> BeLeave's ability to procure services from Aggregate IQ only resulted from the actions of Vote Leave, in providing those donations and arranging a separate donor for BeLeave. While BeLeave may have contributed its own design style and input, the services provided by Aggregate IQ to BeLeave used Vote Leave messaging, at the behest of BeLeave's campaign director. It also appears to have had the benefit of Vote Leave data and/or data it obtained via online resources set up and provided to it by Vote Leave to target and distribute its campaign material. This is shown by evidence from Facebook that Aggregate IQ used identical target lists for Vote Leave and BeLeave ads, although the BeLeave ads were not run.[10]

Finally, the Electoral Commission noted in its report that the evidence does not support the statements of Vote Leave and BeLeave to the effect that the payments BeLeave made to AIQ were donations and that Vote Leave had no influence over the way BeLeave had used them.[11]

Investigation of the United Kingdom Information Commissioner's Office

On 6 November 2018, the U.K. Information Commissioner's Office (ICO) report on its investigation into the use of data analytics in political campaigns was presented in the U.K. Parliament.[12] On the same date, the Information Commissioner, Elizabeth Denham, appeared before the U.K. Committee, to discuss – among other things – the findings of her investigation.[13]

On 11 July 2018, the ICO had released an interim report on the progress of its investigation at the U.K. Committee's request.[14] That same day, the ICO had also published a report containing public policy recommendations stemming from the investigation.[15]

10 Ibid., para. 4.19.

11 Ibid., para. 4.20, p. 20.

12 U.K., Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns A report to Parliament*, 6 November 2018.

13 U.K., Parliament, *Digital, Culture, Media and Sport Committee*, 6 November 2018.

14 U.K., Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns Investigation update*, 11 July 2018.

15 U.K., Information Commissioner's Office, *Democracy disrupted? Personal information and political influence*, 11 July 2018.

On 24 October 2018, the ICO fined Facebook £500,000 for its serious breaches of data protection law.[16] This fine was the result of the ICO's investigation into the use of data analytics in political campaigns. Ms. Denham explained that she decided to impose the maximum fine allowable under the legislation in force at the time because of the seriousness of the accusations against Facebook, and she emphasized that the amount would have been much higher if the *General Data Protection Regulation* (GDPR) had been in force.[17] Indeed, the fine was issued under the *Data Protection Act 1998*, which was replaced in the U.K. in May 2018 by the new *Data Protection Act 2018* and the GDPR, which provide for maximum fines of £17 million or 4% of the fined company's total worldwide annual turnover.[18]

The ICO's findings regarding Facebook that led to the fine – and that pertain to the Committee's study – were severe:

> The ICO's investigation found that between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had.
>
> Facebook also failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform. These failings meant one developer, Dr Aleksandr Kogan and his company GSR, harvested the Facebook data of up to 87 million people worldwide, without their knowledge. A subset of this data was later shared with other organisations, including SCL Group, the parent company of Cambridge Analytica who were involved in political campaigning in the US.
>
> Even after the misuse of the data was discovered in December 2015, Facebook did not do enough to ensure those who continued to hold it had taken adequate and timely remedial action, including deletion. In the case of SCL Group, Facebook did not suspend the company from its platform until 2018.[19]

The report of 6 November includes the results of the ICO's investigation into the links between AIQ, SCL Elections (SCLE) and Cambridge Analytica (CA). The report notes that AIQ explained to the ICO that all of its work had been done with SCLE, not CA. The

16 U.K., Information Commissioner's Office, *ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information*, 25 October 2018. See also the notice of fine: U.K., Information Commissioner's Office, *Data Protection Act 1998 Supervisory Powers of the Information Commissioner Monetary Penalty Notice*, 24 October 2018.

17 U.K., Information Commissioner's Office, *ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information*, 25 October 2018.

18 Ibid.

19 Ibid.

report also states that the ICO's review of the data collected at that stage revealed no evidence that CA had shared personal information, including that of U.K. citizens, with AIQ.[20] The report offers the following conclusion regarding the legal status of AIQ:

> While there was clearly a close working relationship between the entities and several staff members were known to each other, we have no evidence that AIQ has been anything other than a separate legal entity.
>
> We can, however, understand the broader concerns about the close collaboration between the companies which stemmed from shared contact details on company websites and details of payments.[21]

The report establishes that the relationship between AIQ and SCLE was a contractual one and states that no evidence of unlawful activity relating to the personal information of U.K. citizens and AIQ's work with SCLE was found, and that no evidence has been provided to date that these entities were involved in data analytics work with the Brexit referendum campaigns.[22]

According to the first version of the report, these findings were confirmed by the Office of the Privacy Commissioner of Canada (OPC). As regards the investigations into Facebook and AIQ jointly conducted by the OPC and the Office of the Information and Privacy Commissioner for British Columbia (OIPC), which are discussed in more detail later in this chapter, the report states that the Canadian commissioners' offices informed the ICO that they did not find U.K. citizens' personal data, other than that identified within the scope of its enforcement notice.[23] The ICO made corrections to its report and published the following statement on its website: "the report now acknowledges the contribution made by the Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia to the finding regarding UK citizens. Their investigations are ongoing and they have not yet reached a conclusion."[24]

The report states that, in response to an information notice from the ICO, Facebook confirmed that AIQ had created and placed advertisements for the Democratic Unionist

---

20 U.K., Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns A report to Parliament*, 6 November 2018, p. 41.

21 Ibid.

22 Ibid., p. 42.

23 Ibid., p. 43.

24 U.K., Information Commissioner's Office, *Investigation into data analytics for political purposes*.

Party (DUP) Vote to Leave campaign, Vote Leave, BeLeave and Veterans for Britain.[25] The report also notes the following:

> In response to our information notice, Facebook stated that the email addresses did not originate from data collected through Dr Kogan's app but came from a different source.…
>
> Facebook confirmed that Vote Leave and BeLeave used the same data set to identify audiences and select targeting criteria for ads. However, BeLeave did not proceed to run ads using that data set. The Electoral Commission report dated 17 July 2018 confirms that BeLeave did not submit an electoral return.[26]

Commissioner Denham explained that she examined to what extent – and on what basis – AIQ and SCLE had shared the personal information of U.K. voters with each other and with others in order to target the advertising in question. The Commissioner also explained that she had shared the relevant evidence with the Electoral Commission where appropriate. The Electoral Commission was investigating allegations of coordination between Vote Leave and BeLeave and the possible violation of electoral rules, as described in the first part of this chapter.[27]

Regarding the police investigations into this affair, the report reads as follows:

> The Electoral Commission has referred individuals to the police for investigation; those individuals have therefore declined to speak to our enquiry at this time. We will revisit this strand of the investigation for any data protection issues at the conclusion of the police enquiries.[28]

The report explains that, after the ICO issued a revised enforcement notice – which contained specific instructions for AIQ and extended the investigation – on 24 October 2018, the ICO found no evidence of unlawful processing of U.K. personal data.[29]

However, the report points out AIQ's lack of cooperation in the past, which its letter of 5 March 2018 to the ICO had made clear by asserting that AIQ was not subject to the jurisdiction of the ICO and that it considered its involvement in the investigation concluded. Indeed, Commissioner Denham had advised the Committee of this problem

25 Ibid., p. 49.

26 Ibid., p. 50.

27 Ibid.

28 Ibid.

29 Ibid., p. 51–52.

during AIQ's first appearance.[30] The report notes that the situation subsequently improved when AIQ agreed to cooperate fully with the investigation in April 2018.[31]

Regarding the work AIQ did for BeLeave, Veterans for Britain and Vote Leave, the report concludes that no evidence was found that personal information was unlawfully processed, transferred outside the U.K. or processed without the consent of the individuals concerned.[32]

However, the report did include a warning about the actions of Vote Leave:

> we are investigating how Vote Leave delivered electronic marketing communications and whether its actions contravened PECR [Privacy and Electronic Communications Regulations]. We do have cause for concern and we will be reporting on this imminently.[33]

If the ICO releases new information of interest, the Committee reserves the option to reopen this study or to undertake another study on the basis of that new information.

Investigations of the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia

As mentioned earlier and as explained in the Committee's interim report of June 2018, the OPC and the OIPC are conducting joint investigations into Facebook and AIQ.[34]

On 10 May 2018, the Committee heard from the Information and Privacy Commissioner for British Columbia, Michael McEvoy.[35] The Committee heard from the Privacy Commissioner of Canada, Daniel Therrien, on 17 April and 31 May 2018. Mr. Therrien appeared again, on 1 November 2018, at the very end of the Committee's study.

30 Ibid., p. 52. See ETHI, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, p. 18.

31 Ibid.

32 Ibid., pp. 52–53.

33 Ibid., p. 53.

34 ETHI, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, p. 25.

35 Ibid., p. 26.

During his testimony on 1 November, Mr. Therrien stated that work on his joint investigation with the OIPC is proceeding well, but that they have not yet reached any conclusions. They continue to collect and analyze information.

> Our investigation of AIQ focuses on whether it collected or used personal information without consent, or for purposes other than those identified or evident to individuals. Since my last appearance, OPC investigators have issued additional requests for information. They've conducted a site visit. They've undertaken sworn interviews with both Mr. Massingham and Mr. Silvester, and they have reviewed hundreds of internal records from AIQ, including AIQ electronic devices.
>
> In order to make our conclusions public as soon as possible, our plan is to proceed in two phases: one at the end of this calendar year—next month—and a second phase in the spring.[36]

CONCLUSION REGARDING AGGREGATE IQ

Once the findings of the OPC and OIPC regarding this matter are released, the Committee will decide whether it is appropriate to reopen this study or undertake another one on new grounds.

36 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018 (Daniel Therrien, Privacy Commissioner of Canada).

CHAPTER 3: PRIVACY PROTECTION AND POLITICAL PARTIES

APPLICATION OF PRIVACY LAWS TO POLITICAL PARTIES

In its interim report, the Committee recommended that the Government of Canada take measures to ensure that privacy legislation applies to political activities. It heard additional evidence on this topic in the fall.

Point of View of Academics

Fenwick McKelvey, Associate Professor of Communications at Concordia University, supports the Committee's recommendation that privacy laws apply to all political parties. He recommended adopting a code of conduct in order to improve Canadian politics.[37] In his view, not subjecting political parties to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) is a mistake, because doing so would be "a very easy fix, and we see it being effective in [British Columbia]."[38]

Elizabeth Dubois, Assistant Professor in the Department of Communication at the University of Ottawa, pointed out that political entities collect data constantly, not just during election campaigns. She admitted that political entities do not always use data in a harmful way, but suggested that "to balance things we need to make sure we include political parties under the personal data uses laws that we have, PIPEDA being the main one."[39] She added that legislative provisions to ensure transparency and accountability for political uses of personal data are needed.[40]

Ms. Dubois remarked that political parties are not the only ones who should be subject to privacy laws, as they are not alone in collecting certain data. She argued that, since non-profit organizations, unions and other third parties are also collecting data in a

37 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1115 (Fenwick McKelvey, Associate Professor, Communication Studies Concordia University).

38 Ibid., 1140.

39 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1105 (Elizabeth Dubois, Assistant Professor, Department of Communication, University of Ottawa).

40 Ibid.

similar way to political parties, "the questions about how this data is collected and what is the responsible use have to be broader than simply political parties writ large."[41]

Michael Pal, Associate Professor of Common Law in the University of Ottawa's Faculty of Law, emphasized that, while Bill C-76, which would amend the *Canada Elections Act*, is "the biggest step that's been made in terms of political parties and privacy," it does not go far enough. The bill would not give the federal Privacy Commissioner oversight authority, require specific provisions in the privacy policies that political parties must publish or establish an enforcement mechanism.[42]

Mr. Pal pointed out that, in regulating political parties to protect voters' privacy, "we have to actually adapt the content of the rules that are out there for the specific context of political parties and elections."[43]

In addition, Mr. Pal encouraged the Committee members to see privacy regulations as a benefit for political parties. He acknowledged that being regulated is often seen as being onerous and costly, but invited the Committee members to "imagine what would happen if there was a hack of one of Canada's major political parties." Mr. Pal argued that it would not take many hacks or disclosures of personal information held by a political party for the public to lose faith in that party or the entire system.[44]

Point of View of Political Parties

Appearing before the Committee, the Liberal Party of Canada (LPC), the Conservative Party of Canada (CPC) and New Democratic Party of Canada (NDP) underscored their commitment to privacy protection. The parties confirmed that they:

- have adopted a privacy policy that must be followed by all volunteers, party employees and contractors, if any;[45]

41 Ibid.

42 Ibid., 1110 (Michael Pal, Associate Professor, Faculty of Law, Common Law Section, University of Ottawa).

43 Ibid.

44 Ibid., 1150.

45 ETHI, *Evidence*, 1st Session, 42nd Parliament, 30 October 2018, 1100, 1105, 1110, 1115, 1120, 1140 (Trevor Bailey, Privacy Officer and Director of Membership, Conservative Party of Canada; Michael Fenrick, Constitutional and Legal Advisor, National Board of Directors, Liberal Party of Canada; Jesse Calvert, Director of Operations, New Democratic Party).

- do not sell, rent or share the personal information about voters that they possess with third parties;[46]
- use segmented databases to ensure that volunteers and employees have access only to the information they need to complete their tasks;[47]
- use cybersecurity systems to protect the personal information in their possession;[48]
- do not purchase data, other than data from InfoCanada or Canada Post (a phone book and a postal address list);[49] and
- offer personal data protection training at all levels of their organization.[50]

The parties take different positions with respect to the application of privacy laws to political parties.

Michael Fenrick, Constitutional and Legal Adviser to the LPC National Board of Directors, noted that responsible use of data can significantly increase participation and mobilization in the political process and that the interests of political parties differ from those of commercial businesses. As he argued, "It would be a real disincentive to participation in the political process if people could face the kinds of penalties that exist for corporations, for instance, for non-compliance under PIPEDA."[51] The LPC does not support extending the application of PIPEDA in its current form to political parties, as "it's intended to address commercial activity. It's not intended to address political activity."[52]

Trevor Bailey, Privacy Officer and Director of Membership at the CPC, stated that the CPC operates in accordance with its privacy policy, which currently does not allow the CPC to be fully compliant with PIPEDA. He did not wish to take a position on whether political parties should be subject to privacy laws or whether the Privacy Commissioner should

46 Ibid., 1100, 1145, 1200 (Trevor Bailey); Ibid., 1105, 1145 and 1200 (Michael Fenrick); Ibid., 1145 and 1200 (Jesse Calvert).

47 Ibid., 1120 (Trevor Bailey); Ibid., 1110 and 1125 (Michael Fenrick), Ibid., 1115 and 1125 (Jesse Calvert).

48 Ibid., 1100 and 1120 (Trevor Bailey); Ibid., 1105 and 1125 (Michael Fenrick), Ibid., 1115 and 1125 (Jesse Calvert).

49 Ibid., 1135 (Trevor Bailey, Michael Fenrick and Jesse Calvert).

50 Ibid., 1210 (Trevor Bailey, Michael Fenrick and Jesse Calvert); Ibid., 1215 (Michael Fenrick and Jesse Calvert).

51 Ibid., 1130 (Michael Fenrick).

52 Ibid., 1215 (Michael Fenrick).

have oversight authority over political parties' activities.[53] However, he did say that, "if there's a new rule basis that comes in and takes effect for how we need to operate," the CPC would comply with it, but that this "would require significant consultation and development or redesign of our processes."[54]

Jesse Calvert, Director of Operations at the NDP, stated unequivocally that the federal government should extend the application of PIPEDA to political parties. He explained that the NDP believes that Canadians deserve to have trust in their political parties and that transparency is the only way to strengthen that trust. He argued that all political parties should follow the same rules and that oversight of the implementation of internal party policies is possible.[55]

Point of View of the Chief Electoral Officer

The Chief Electoral Officer, Stéphane Perrault, expressed his support for the Committee's interim report recommendation that political parties be subject to basic privacy rules.[56] He contended that, while Bill C-76 would require parties to publish their privacy policy, the bill has three flaws: it provides no minimum privacy standards; it does not institute oversight by an independent body; and it is silent on whether political parties should offer Canadians a way to validate and correct any information they possess about them.[57]

Mr. Perrault recognized that the ability of political parties to obtain the information they need to contact voters is a fundamental part of our electoral system. However, he believes that oversight of their collection and use of personal information is necessary. He argued that privacy principles, in areas such as consent and the way consent is obtained, can be adapted to the unique role that political parties play.[58]

In addition, Mr. Perrault said that he believes the Privacy Commissioner is the right person to carry out this oversight. He also maintains that the privacy policies the parties

53 Ibid., 1130 (Trevor Bailey).

54 Ibid., 1130 and 1215 (Trevor Bailey).

55 Ibid., 1135 (Jesse Calvert).

56 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1135 (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

57 Ibid.

58 Ibid., 1145.

would have to publish under the *Canada Elections Act* if Bill C-76 becomes law should be subject to oversight by the Privacy Commissioner.[59]

Point of View of the Privacy Commissioner

The U.K. Information Commissioner recently reported to the U.K. Parliament on its investigation into the use of data analytics in political campaigns. The report states that her investigators conducted interviews with the 11 main political parties in the U.K. in order to review the way they collect and use personal information. The investigators also learned about the measures parties take to comply with data protection laws. Following the investigation, the U.K. Information Commissioner concluded that the political parties' handling of personal information poses risks. She sent warning letters to the parties asking them to submit data protection impact assessments for all projects involving the use of personal information. The parties have to report back to the Information Commissioner's Office within three months. They were also advised that they will be audited in January 2019.[60]

None of the above is possible in Canada. The OPC has absolutely no oversight authority over the privacy practices of political parties.

Mr. Therrien appeared before the Committee on 1 November 2018. He noted that a recent survey conducted by his office revealed that 92% of Canadians want political parties to be subject to privacy laws. He pointed out that, in September 2018, privacy commissioners from across Canada adopted a joint resolution calling on governments to ensure that political parties are subject to privacy laws. He explained that academic experts, civil society, the Canadian public and the Chief Electoral Officer all support their position. Yet the government maintains that, while the issue should be studied, the next federal election can take place before such measures are enacted.[61]
Mr. Therrien summarized the problem as follows:

> Canadian political parties' lack of oversight is unfortunately becoming an exception compared to other countries, and it leaves Canadian elections open to the misuse of personal information and manipulation.

59 Ibid., 1210.

60 *Investigation into the use of data analytics in political campaigns A report to Parliament*, pp. 23–24.

61 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1120 (Daniel Therrien, Privacy Commissioner of Canada).

> The bottom line is that without proper data regulation, there are important risks to a fair electoral process; and this applies to the next federal election in Canada.[62]

In response to the LPC's argument about the deterrent effect that subjecting political parties to PIPEDA would have because of the penalties that could be imposed, Mr. Therrien expressed surprise. He explained that, while there are penalties for certain specific behaviour, including, as of 1 November 2018, failing to disclose breaches, in general, "PIPEDA suffers from lack of enforcement."[63]

Mr. Therrien added that, to his knowledge, "it has not been borne out where these laws apply, and I have not seen evidence … that the quality of the communication would be impaired if political parties were subject to privacy laws."[64] He also commented that, if PIPEDA were to apply to political parties, he would not hesitate to consider the context in which they operate.

> First, when I recommend that PIPEDA be applied to federal political parties, it is implicit that context would matter. PIPEDA has a number of principles, such as the right to access information and the right to be clear on the purposes for which information would be used by an entity subject to PIPEDA. The fact that we would be dealing with political parties that have legitimate interests, if not rights, to engage in political discussion with electors would be part of the context.
>
> As we would eventually look at the application of PIPEDA to political parties, certainly there could be an examination of enforcement mechanisms, the amount of penalties and what would make sense for the various entities that are subject to it.[65]

However, Mr. Therrien said that, in British Columbia, the enforcement mechanisms are the same for all entities subject to the *Personal Information Protection Act*. He also pointed out that the GDPR and the legislation in British Columbia apply to political parties despite their unique operating environment.[66] Finally, he said that, as far as he knows, no jurisdiction has enacted a separate law to regulate political parties.[67] Mr. Therrien stated that the time for self-regulation has passed.

> The government can delay no longer. Absent comprehensive reform, Parliament should ensure the application of meaningful privacy laws to political parties. It should also give

62 Ibid., 1220.

63 Ibid., 1230.

64 Ibid., 1245.

65 Ibid., 1230.

66 Ibid.

67 Ibid.

> my office the same inspection and enforcement powers that most of Canada's trading partners enjoy.[68]

Finally, like Ms. Dubois, Mr. Therrien argued that political parties are not the only entities that should be subject to privacy laws. Rather, "the act should apply to all organizations engaged in commercial or other activities that compile, use or transmit personal information," including non-profit organizations and third parties.[69]

The Committee is of the opinion that public trust would be better served if privacy laws were to apply to political parties and political third parties (as defined in section 349 of the *Canada Elections Act*). Considering the evidence heard, the Committee reiterates the preliminary recommendation on this subject in its interim report, recommendation 8 (recommendation 26 in this report), and proposes new and more specific recommendations with respect to political parties. The Committee also reiterates recommendation 5 of its interim report, which called for additional audit powers for the Privacy Commissioner (recommendation 23 in this report). Finally, it proposes new recommendations regarding political third parties.

Recommendation 1 on the application of privacy legislation to political parties:

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* in order to subject political parties to it, taking into account their democratic outreach duties.

Recommendation 2 on the application of privacy legislation to political third parties:

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* in order to subject political third parties to it.

Recommendation 3 on personal information protection oversight powers over political parties and political third parties:

That the Government of Canada grant the Office of the Privacy Commissioner and/or Elections Canada the mandate and authority to conduct proactive audits on political parties and political third parties regarding their privacy practices and to issue orders and levy fines.

68 Ibid., 1220.

69 Ibid., 1255.

Recommendation 4 on the financial resources of the Office of the Privacy Commissioner:

That the Government of Canada provide necessary new resources to the Office of the Privacy Commissioner, so it can address modern privacy concerns and efficiently exercise the additional powers granted to the Commissioner.

USE OF FOREIGN FUNDS IN CANADIAN ELECTIONS

Researcher and writer Vivian Krause highlighted problems involving the use of foreign funds to finance environmental and electoral activism in Canada. Ms. Krause argued that the Charities Directorate of the Canada Revenue Agency (CRA) is not properly enforcing the *Income Tax Act* with respect to the registration of charitable organizations.[70] She offered a few examples of American organizations that would have helped fund and direct the activities of Canadian charities that were active in the 2015 federal election. She contended that some of these organizations are illegitimate charities that are simply used to "Canadianize" funds.[71]

Ms. Krause said that, while Bill C-76 would stop all foreign money from entering Canada, it would not prevent funds from being "Canadianized."[72] She said that the best way to protect Canada's elections is for the CRA to enforce the law.

In response to concerns about foreign funding, Mr. Perrault noted the following:

> Bill C-76 would significantly expand the third-party regime and include measures that aim to eliminate opportunities for foreign funds to be used in Canadian elections. This includes an anti-avoidance clause and a ban on the sale of advertising space to foreign entities.[73]

Mr. Perrault emphasized that Bill C-76 addresses two weaknesses of the *Canada Elections Act*.

> The first is that in the past, contributions were made six months prior to the writ period. Because of the way the law is drafted, they were treated as belonging to the entity, so it's their own resources, even though they may come from abroad. The second

70 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1130 (Vivian Krause, Researcher and Writer).

71 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1135 (Vivian Krause).

72 Ibid., 1255.

73 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1130 (Stéphane Perrault).

> weakness is that the current law regulates election advertising, which is a narrow category of expenditures.
>
> …
>
> On both fronts, Bill C-76 improves that by expanding it to all partisan activities and requiring a reporting of all contributions. It also has a number of additional measures. One of them I recommended at committee, which is having an anti-avoidance clause precisely to deal with the kind of situation where money is being passed from one entity to another and claims are made Canadian in the process.[74]

As for communication between the CRA and Elections Canada, Mr. Perrault explained that this issue is less his responsibility than that of the Commissioner of Canada Elections.[75]

One of the organizations targeted by some of Ms. Krause's comments is Tides Canada. Andrew Heitzman, Chairman of the board of directors of Tides Canada, has provided the Committee with a letter responding to allegations made by Ms. Krause. In this letter, he stresses that Tides Foundation in the United States and Tides Canada are separate organizations. He further explains:

> Ms. Krause claimed that Tides Canada has been involved in directing donations to non-charities, for political or other purposes. These assertions are untrue, defamatory, and appear to be based on a lack of knowledge or outright misrepresentations regarding the legal framework for Canadian charities. Tides Canada does not make grants to non-charities for any purpose and has never supported, directly or indirectly, through making grants or other means, any political party, politician, or candidate for office.
>
> Ms. Krause continues to misrepresent our work and the information that we make publicly available about our activities. Tides Canada is a well-respected and professionally managed organization that is fully compliant with the laws and policies governing charities in Canada. A thorough Canada Revenue Agency audit of Tides Canada Foundation was successfully concluded in 2016, and the organization remains a registered charity in good standing with CRA. Tides Canada is also accredited under the Imagine Canada standards program, which recognizes excellence in charity governance, accountability, and transparency[76].

The Committee agrees that the federal government should ensure that foreign funds are not used to influence Canadian elections and makes the following recommendation:

---

74 Ibid., 1150.

75 Ibid., 1155.

76 Letter to the Members of the Committee from Andrew Heintzman, Chair of the Board of Directors of Tides Canada, 15 November 2018.

Recommendation 5 on the foreign funding of political activities:

That the Government of Canada take all steps to prevent the foreign funding and influence in domestic elections, including foreign charitable funding.[77]

77 Bill C-76 is currently before the Senate and may address this issue if adopted in its current version.

CHAPTER 4: REGULATION OF SOCIAL MEDIA PLATFORMS IN THE ERA OF DISINFORMATION AND MISINFORMATION

COUNTERING THE SPREAD OF ONLINE DISINFORMATION AND MISINFORMATION

The Committee repeatedly heard about problems with social media platforms that allow or facilitate the spread of disinformation and misinformation. The Committee identified three important issues to consider: the nature of the digital information ecosystem, the very structure of social media platforms and the problems with self-regulation.

Transformation of the Information Ecosystem

The era when the only ways for people to learn the news were to listen to the radio, read a print newspaper or watch a live news broadcast is long past. Today, a vast amount of content is available online, and the publishers of the past have been replaced by artificial intelligence (AI).

Mr. Taylor Owen, Assistant Professor of Digital Media and Global Affairs at the University of British Columbia, explained that, until the emergence of the social Web and the decline of the traditional media, responsibility for maintaining acceptable discourse was the prerogative of a small number of 20th-century media institutions that "perpetuated an economic system, and arguably a political system, that benefited certain groups over others."[78] Public discourse was therefore limited, and people did not hear everyone's opinions the way they do today. When the social Web appeared, debate in the public sphere became "much more diverse, much more dynamic, and much more informative than had been mitigated by that legacy media infrastructure."[79]

However, developments in social media in recent years have created a new structure that determines what is acceptable and sets the boundaries on public debate: the platforms' filtering mechanisms, which decide what people see and whether our content

78 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1130 (Taylor Owen, Assistant Professor, Digital Media and Global Affairs, University of British Columbia).

79 Ibid.

will be seen. Mr. Owen asserted that Canadians should be concerned about filtering by algorithms and the business models that determine the content that people see.[80]

Ben Scott, Director of Policy and Advocacy at the Omidyar Network, compared the purchase of a magazine from a newsstand in an airport, where the consumer can see the full range of magazines available for sale in various subject areas (politics, gardening, sports, etc.), with the way information is consumed online to illustrate the difference between the traditional media and the digital environment.[81]

> In the digital environment, all of that is compressed into a single stream, and it looks the same. It's a Facebook newsfeed. It's a Twitter feed. It's a YouTube NextUp list of videos. In that environment, all of the signals about source credibility and quality that we once had begin to attenuate.
>
> …
>
> We've lost the normative structure that in the old media environment allowed us as citizens to make implicit judgments about source credibility and, when we're reading digital media, to engage in critical thinking.[82]

Ms. Dubois identified another problem with the new information ecosystem: in the old media system, spreading disinformation cost a lot of money and required a lot of resources; now, it is easy to do.[83]

Besides the challenges of the current information ecosystem, social media platforms also have inherent structural problems.

Structural Problems with Social Media Platforms

Mr. Owen believes that the vulnerabilities revealed by the breach are not the result of isolated malicious individuals but rather "a function of structural problems in our very digital infrastructure, which … are creating weaknesses in our free and open society."[84] He explained that we now live in the platform era, in which the Internet is controlled by a small number of global platform companies. This platform Internet has two intrinsic

80 Ibid.

81 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1125 (Ben Scott, Director, Policy and Advocacy, Omidyar Network).

82 Ibid.

83 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1200 (Elizabeth Dubois).

84 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1100 (Taylor Owen).

structural problems: the monetization of the platforms, which is also known as the attention economy, and the fact that the character of the digital ecosystem and the user experience are increasingly determined "by unaccountable artificial intelligence systems."[85]

Mr. Owen reported that the monetization of the platforms requires commercializing our attention and behavioural changes.

> [P]latform algorithms prioritize entertainment, shock, and radicalization over reliable information. This is embedded in the business model. This is why research shows, for example, that misinformation spreads further and faster than genuine news.[86]

As for the AI used to "filter the most engaging content to us, to know what will rile us up and engage us, to determine what we see as an individual user and whether we are seen and heard inside these platforms," Mr. Owen stated that it serves to create various versions of reality that specifically target each individual, which are sometimes called "deep fakes" or "synthetic media."[87]

Mr. Owen explained that the structural problems with social media platforms are responsible for the negative externalities observed in democracy.[88] These externalities include fragmentation and the vulnerability of elections. Mr. Owen described how each user is served a customized diet of information designed to reinforce and harden their views. This fragmentation means that "polarization and tribalism can very quickly emerge," and it is "increasingly leading to actual physical manifestations of individual and collective violence."[89] Regarding the vulnerability of elections, he said that foreign countries can use the tools of the attention economy to influence voter behaviour (e.g., microtargeting, cyberattacks and hacking).[90]

Mr. Scott called the "politics of resentment that we're seeing in contemporary populism mixed with the distorting power of the digital information market" a "toxic brew."[91] Mr. McKelvey noted that algorithms are not always effective at recognizing good-quality or credible information. Information sorting is carried out using a market-based

85 Ibid.

86 Ibid., 1100.

87 Ibid.

88 Ibid., 1105.

89 Ibid.

90 Ibid.

91 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1120 (Ben Scott).

approach rather than with a focus on content quality.[92] Claire Wardle, Executive Chair of First Draft, a non-profit organization housed at the Shorenstein Center on Media, Politics and Public Policy of Harvard University's Kennedy School, stated that people look for information, consume it and share it based on their emotions. She confirmed that the algorithms used by social media platforms reflect this fact. The more people engage with content, the more likely it will go viral. The problem is that deceptive content is often what generates the strongest reactions and is being promoted.[93]

Tristan Harris, Co-Founder and Executive Director of the Center for Humane Technology, believes that technology is no longer designed to suit human capacities. Instead, it is creating distortions that are starting to bend and break our conception of reality. According to Mr. Harris, because people are constantly using their electronic devices every day, their thoughts are now being generated by what they see on screens, and that is a form of psychological influence.[94] Self-optimizing AI systems use algorithms to predict the best content to suggest to a given individual, and the personalization of user accounts enables billions of people to be targeted by personalized forms of manipulation. He argues that technology companies have an ethical decision to make: redesign their products and realign the way technology works to account for the limits of human beings to make sense of the world and make choices, or do nothing and face the consequences.[95]

Mr. Harris argued that social media platforms' manipulation of people can have negative effects. For example, it can have a harmful impact on children who consume online content. Unlike traditional media, which are regulated (e.g., they are prohibited from showing certain content on Saturday mornings and must use a five-second delay), online media are unfiltered. Mr. Harris noted the following:

> [W]hen the engineers at Snapchat or Instagram—which, by the way, make the most popular applications for children—go to work every day, these are 20- to 30-year-olds, mostly male, mostly engineers, computer science or design-trained individuals, and they don't go to work every day asking how they protect the identity development of children.… The only thing they do is go to work and ask, "How can we keep them hooked? Let's introduce this thing called a 'follow button', and now these kids can go

92 Ibid., 1205 (Fenwick McKelvey).

93 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1105 and 1140 (Claire Wardle, Research Fellow, Shorenstein Center on Media, Politics and Public Policy, Kennedy School, Harvard University).

94 Ibid., 1120 (Tristan Harris, Co-Founder and Executive Director, Center for Humane Technology).

95 Ibid., 1125.

> around following each other. We've wired them all up on puppet strings, and they're busy following each other all day long because we want them just to be engaged."[96]

Mr. Harris described how, as competition in the attention economy intensifies, social media platforms can no longer wait for users to choose to use the product. They now have to reach down the brain stem and make people addicted to it, creating an unconscious habit.[97] The business model of data companies is to accumulate as much personal information about their users as possible and to manipulate them. As a result, there is no fair exchange between the two parties.[98] For example, he pointed out that YouTube is not obligated to suggest content on the right side of the screen. It does so because its business model is to maximize engagement with the platform. The problem results mainly from the advertising-supported engagement business model.[99]

Mr. Harris said that the question is at what point publishers are responsible for the content they transmit. He believes it makes sense for technology companies not to be responsible for the industrial amount of content that people post to their platforms. However, when the content is fuelled by recommendations generated by the platforms, using AI that they have programmed, (e.g., Alex Jones videos that were recommended 15 billion times on YouTube), they should perhaps be held responsible for publishing those recommendations.[100] By making them responsible for their business model, that model would become more costly.

> Right now we have dirty-burning technology companies that use this perverse business model that pollutes the social fabric. Just as with coal, we need to make that more expensive, so you're paying for the externalities that show up on society's balance sheet, whether those are polarization, disinformation, epistemic pollution, mental health issues, loneliness or alienation. That has to be on the balance sheets of companies.[101]

Ms. Dubois seemed to agree with Mr. Harris. She asserted that there is an important distinction between "allowing content to exist" and "being responsible for that content, and being responsible for what content shows up as trending topics, recommended search results or something that is at the top of people's newsfeeds."[102] Platforms make

96 Ibid., 1155.

97 Ibid., 1200.

98 Ibid., 1220.

99 Ibid., 1215 and 1230.

100 Ibid., 1205.

101 Ibid., 1230.

102 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1145 (Elizabeth Dubois).

decisions about what will or will not be highlighted. These decisions should be made based on whether they will silence groups that should not be silenced or promote content that should not be published or promoted.[103]

The structural problems inherent in social media platforms serve to fuel the attention economy and help in the promotion of disinformation and misinformation to millions of addicted users. The Committee is very concerned about the negative externalities these platforms have.

Inadequacy of Self-Regulation

The Privacy Commissioner described the current situation in alarming terms.

> Last week, I attended the 40th international conference of data protection and privacy commissioners, in Brussels. The conference confirmed what I had explained in my last annual report: There is a crisis in the collection and processing of personal information online. Even tech giants … are recognizing that the status quo cannot continue.
>
> Apple CEO Tim Cook spoke of "a data industrial complex" and warned that "[o]ur own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency"…. Facebook's Mark Zuckerberg admitted that his company committed a serious breach of trust in the Cambridge Analytica matter. Both companies expressed support for a new U.S. law that would be similar to Europe's General Data Protection Regulation or GDPR.
>
> When the tech giants have become outspoken supporters of serious regulation, then you know that the ground has shifted and we have reached a crisis point.
>
> …
>
> The government, however, has been slow to act, thereby putting at continued risk the trust that Canadians have in the digital economy, in our democratic processes and in other fundamental values.[104]

Mr. Therrien also underscored the importance of privacy:

> Individual privacy is not a right we simply trade off for innovation, efficiency or commercial gain. No one has freely consented to having their personal information weaponized against them…. Similarly, we cannot allow Canadian democracy to be

103 Ibid.

104 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1215 (Daniel Therrien).

> disrupted, nor can we permit our institutions to be undermined in a race to digitize everything and everyone simply because technology makes this possible.[105]

Mr. Owen stated that, when largely unregulated monopolies create negative externalities, governments must intervene to protect the collective interest.[106] He believes that a comprehensive policy approach is needed to reform the way social media platforms are regulated and change people's relationship with the digital economy as a whole.[107]

Likewise, Mr. Scott argued that the private sector cannot be relied upon to resolve the problem: "Publicly traded monopolies do not self-regulate." He believes the answer is the government "using its tools to steer the market back in the direction of the public interest." For example, he suggested adopting a digital charter for democracy that would lay out a set of principles and establish clear policies to produce the changes required to protect the integrity of the democratic public sphere.[108]

Ms. Dubois stated that self-regulation is not effective for the large platforms. She believes that these businesses must be held responsible for the content they post on their platforms and be transparent and accountable in regards to the manipulation of data they conduct. Ms. Dubois explained that, right now, they are a "black box." She said, "We don't know how Facebook or Google decides what shows up and what doesn't."[109] She identified another important reason why Canada should regulate social media platforms: most of them are large global corporations that are not necessarily familiar with the unique characteristics of Canadians when they design their self-regulation.[110]

Risks Associated with Regulation

Despite the above, some witnesses had reservations about the regulation of social media platforms.

For example, despite confirming that Google has taken the measures necessary to comply with the GDPR, Colin McKay, Head of Public Policy and Government Relations at

105 Ibid., 1220.

106 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1110 (Taylor Owen).

107 Ibid., 1110.

108 Ibid., 1120 (Ben Scott).

109 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1105 (Elizabeth Dubois).

110 Ibid., 1235.

Google Canada, pointed out that "the extension of GDPR … would create greater compliance obligations on smaller and medium-sized businesses," which, around the world, are already feeling the "stress … of understanding their obligations under the GDPR."[111] Regarding the possibility that independent auditors visit Google offices to verify that it is using its algorithms appropriately, Mr. McKay said, "In some cases the algorithm is proprietary commercial technology, and I don't know if an auditor would have the capacity to evaluate what the algorithm is intended to do, or how they would evaluate working versus non-working and under what standard."[112]

As for the option of establishing an independent public body to administer and make decisions about the right to be forgotten and privacy in cases of defamation, harassment or hate (rather than letting the platforms make them), Mr. McKay pointed out that content removal could conflict with freedom of expression. He argued that the best solution is to use the courts, which understand both the applicable norms and the public's expectations. He appeared to doubt the legitimacy of the idea of charging an administrative tribunal with deciding freedom of expression issues.[113]

Oath Inc. (Oath), a subsidiary of Verizon that includes a number of digital platforms, including AOL, Yahoo and Tumblr, submitted a brief to the Committee. The brief discusses Oath's practices and states that it supports industry self-regulation. Oath agrees that self-regulation is not a privacy panacea, but believes that it ensures an ecosystem of cooperative compliance. The company supports industry self-regulation for digital advertising, including through the Digital Advertising Alliance Canada.[114]

Samantha Bradshaw, a researcher who is involved in the Oxford Internet Institute's Computational Propaganda project, also expressed concerns about excessive regulation and the risk that regulations requiring the removal of content from social media platforms could end up suppressing important elements of democratic debate.[115] Mr. Pal echoed these comments, noting that "we want to facilitate political expression. We don't want to restrict that. Some of the potential laws you could come up with might restrict political expression."[116]

---

111 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 October 2018, 1205 and 1215 (Colin McKay, Head, Public Policy and Government Relations, Google Canada).

112 Ibid., 1245.

113 Ibid., 1250.

114 Oath Inc., *Brief*, p. 6.

115 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1125 (Samantha Bradshaw).

116 Ibid., 1145 (Michael Pal).

The Committee has taken the comments from industry representatives and some academics into account, but still believes that some type of regulation is necessary.

POTENTIAL REGULATORY SOLUTIONS

Transparency in Online Advertising

A number of witnesses discussed the need for more transparency in the advertising placed on social media platforms. For example, Mr. Scott maintained that there is "no reason in the world why every citizen who sees a political ad shouldn't know exactly who bought it, how much they spent, and how many people they paid to reach."[117] He believes that voters should also know why they are seeing a particular message so that they can look at political advertising with a more critical eye.[118] Mr. Scott suggested that a little box should pop up when individuals move their electronic device's cursor over an online advertisement and provide information about the ad, such as "who bought the ad; how much they paid for it; how many people have seen it besides you; and, most importantly, why you got that ad—what the demographic features were that were chosen by the advertiser to make that ad come to you."[119]

Mr. Scott further proposed that "all the politicalized ads that come up on Facebook or Twitter or Google ought to be in a database that is publicly accessible." This database would enable the public to see what kinds of messages are being delivered to various target audiences and whether they vary from one audience to another.[120] The database should be accessible to journalists and researchers and have a simple user interface that offers easy access to the data and allows the ads to be reviewed so that people can understand how political propaganda works.[121] Some businesses announced that they would create transparency databases, but Mr. Scott reported that these databases do not meet the desired standard. In his view, legislation will be required to achieve that standard.[122]

117 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1125 (Ben Scott).

118 Ibid.

119 Ibid., 1150.

120 Ibid.

121 Ibid.

122 Ibid., 1155.

The other challenge Mr. Scott identified is the definition of "political advertising," which differs from platform to platform.[123] Ms. Wardle made a similar point, underlining the importance of not defining what is considered a political ad too narrowly:

> If any type of policy or even regulation applies simply to ads that mention a candidate or party name, we would be missing the engine of any disinformation campaign, which is messages designed to aggravate existing cleavages in society around ethnicity, religion, race, sexuality, gender and class, as well as specific social issues.[124]

She supports the creation of a central public database of political ads that uses machine-readable formats and is updated in real time.[125]

Mr. Pal said it would be a good idea to create a public repository of all election-related ads. He acknowledged that Facebook has recently done that voluntarily, but the company could reverse course at any time. This repository would therefore need to be legally mandated.[126] Mr. Pal also emphasized that, while the *Canada Elections Act* and the related legislation govern political parties, leadership candidates, nomination contestants and third parties, these laws should also explicitly regulate social media platforms and technology companies. These platforms should be required to disclose and maintain records about the source of any entities attempting to post political advertising on them.[127]

Mr. Perrault noted that Bill C-76 would require social media platforms to publish and retain a registry of election advertising and partisan advertising, which would improve transparency. The bill would also clarify and expand the current provisions that address some kinds of online impersonation and certain false statements about candidates.[128]

Mr. Owen argued for total transparency that is not limited to political advertising. He believes that, both as consumers in the context of consumer protection and as voters in the context of election integrity protection, we should have the right to know how we

123 Ibid.

124 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1105 (Claire Wardle).

125 Ibid., 1105, 1140.

126 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1115 (Michael Pal).

127 Ibid., 1110.

128 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1130 (Stéphane Perrault).

are "being microtargeted using incredibly sophisticated systems to target and nudge our behaviour."[129]

Regarding transparency in online advertising, the Committee recognizes that Bill C-76 will bring important measures, including an obligation for social media platforms to publish and keep a registry of all political and partisan advertisements. However, some testimony suggests that registries that have already been set up by social media platforms are not user-friendly and easily searchable. The Committee therefore recommends an additional measure to supplement what is already provided for in Bill C-76:

Recommendation 6 on political advertising:

That the Government of Canada amend the *Canada Elections Act* to require an authorizing agent to submit identification and proof of address when placing political ads online.

Recommendation 7 on the creation of an online political advertising database:

That the Government of Canada amend the *Canada Elections Act* to require social media platforms to create searchable and machine-readable databases of online political advertising that are user-friendly and allow anyone to find ads using filters such as: the person or organization who funded the ad; the political issue covered; the period during which the ad was online; and the demographics of the target audience.

The Committee further reiterates recommendation 1 of its interim report on transparency (recommendation 19 of this report).

Algorithmic Transparency and Responsibility for Content

Mr. Scott believes that there needs to be a review of how algorithms used by social media platforms work and how they impact social welfare. There needs to be an understanding of the weaknesses that allow them to be weaponized to be able to avoid these strong negative effects.[130] Mr. Owen gave an example of legislation recently passed in California that, as of June 2019, would force all automated accounts to self-identify as being automated.[131] He acknowledges that "[t]here are all sorts of potential

129 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1200 (Taylor Owen).

130 Ibid., 1125 and 1135 (Ben Scott).

131 Ibid., 1135 (Taylor Owen).

positive uses of bots and automated tools in the social ecosystem." He believes, however, that as consumers, Canadians should know whether they are being targeted by one of these bots.[132]

With regard to algorithmic transparency, Ms. Dubois recommended the following:

> For example, we could have clearer testing processes, where data is open for government and/or academics to double-check procedures. There could be regular audits of algorithms, the way financial audits are required, and documented histories of the algorithm development, including information about how decisions were made by the team and its members and why. We also need things like clearer labelling of automated accounts on social media or instant messaging applications, and registrations of automated digital approaches to voter contact. You could imagine a voter contact registry being modified to include digital automated approaches.[133]

She added that it would be good to be able to look at a history of the decisions of the team who made the algorithm in the first place. That would provide information about what it was supposed to do, and why and how.[134]

Ms. Bradshaw said that if it were possible to look at the actual principles that go into the algorithmic design (e.g., the information's virality) and replace them with principles that would support a better democracy, such as "principles on factual information coming from professional news outlets as opposed to sources that constantly produce misleading or fake news," it would be possible to regulate the platforms in ways that would not harm free speech. She suggested for example that perhaps professional news should be prioritized in the algorithms.[135]

Ms. Wardle spoke about the need for more transparency around the behaviours of social media platforms and the decisions they make, such as those regarding content automation.[136]

In light of this evidence, the Committee makes the following recommendations regarding algorithmic transparency and social media platforms' responsibility for online content:

---

132 Ibid.

133 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1105 (Elizabeth Dubois).

134 Ibid.

135 Ibid., 1225 (Samantha Bradshaw).

136 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1215 (Claire Wardle).

Recommendation 8 on regulating certain social media platforms:

That the Government of Canada enact legislation to regulate social media platforms using as a model the thresholds for Canadian reach described in clause 325.1(1) of Bill C-76, An Act to amend the Canada Elections Act and make certain consequential amendments. Among the responsibilities should be included a duty:

- **to clearly label content produced automatically or algorithmically (e.g. by 'bots');**
- **to identify and remove inauthentic and fraudulent accounts impersonating others for malicious reasons;**
- **to adhere to a code of practices that would forbid deceptive or unfair practices and require prompt responses to reports of harassment, threats and hate speech and require the removal of defamatory, fraudulent, and maliciously manipulated content (e.g. "deep fake" videos); and**
- **to clearly label paid political or other advertising.**

Recommendation 9 on algorithmic transparency:

That the Government of Canada enact transparency requirements with respect to algorithms and provide to an existing or a new regulatory body the mandate and the authority to audit algorithms.

The Committee wishes to specify that the monetary sanctions imposed by the new proposed legislative measures should represent more than the mere cost of doing business for a company.

Content Moderation

Mr. Scott said that citizens should have a right to be protected from illegal content. Hate speech, defamation, harassment, and incitement to violence are all considered illegal in the off-line world. He believes that such content should also be considered illegal in the online world and quickly taken down from social media platforms using a "process that is rigorously overseen by regular judicial oversight and that has an appeals process so that we are not endangering freedom of expression." He believes that while the power

to take down illegal content must not be ceded to social media platforms, their involvement is needed to speed up the process.[137]

Ms. Bradshaw also discussed content moderation, citing as an example Myanmar and the way Facebook was used to spread disinformation that led to violence against the Rohingya, the Islamic minority in that country. She believes that this case illustrates the fact that social media platforms operate on a global scale, but they do not necessarily have staff that is sensitive to the realities of each country to be able to moderate content pertaining to local issues. She encourages content moderation that is more global and inclusive to prevent having a content moderator in California making decisions on content in countries where there are ethnic tensions, for example.[138]

Recommendation 10 on the taking down of illegal content by social media platforms:

That the Government of Canada enact legislation imposing a duty on social media platforms to remove manifestly illegal content in a timely fashion, including hate speech, harassment and disinformation, or risk monetary sanctions commensurate with the dominance and significance of the social platform, and allowing for judicial oversight of takedown decisions and a right of appeal.

User Control and Consent

Mr. Scott referred to provisions in the GDPR to discuss the importance of consent. There is a provision in the GDPR that now bans confidentiality agreements that do not give people a real choice regarding control over their own data. Confidentiality agreements like the one used by Facebook, which are all or nothing (if I agree to sign, I can access a platform used by two billion people; if I do not, I abandon all Facebook services), are no longer allowed. Mr. Scott believes that consumers need to be given control over the data collected about them and how it is used. For Mr. Owen, certain principles, such as consent and the right to be informed, are protections against the misuse of this personal data.

> If we consent regularly to the use, sharing and amalgamation of our personal data—if we have the right to that consent—and if we have the right to know how that data is being used, whether it's for psychographic profiling, for an AI-driven microtargeting campaign, or for whatever reason, that protects us and inoculates us against the

137 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1125 (Ben Scott).

138 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1230 (Samantha Bradshaw).

> potential risk of these technologies in the future, not how they were used in one moment of time by one group.[139]

Mr. Therrien said that new Canadian legislation should place a heavy emphasis on meaningful consent. It should also consider other ways to protect privacy where consent may not work, for instance in the development of artificial intelligence. In this respect, he noted that the GDPR concept of legitimate interest may be considered.[140]

The Committee reiterates recommendation 2 in its interim report, which aims at implementing measures that are similar to those contained in the GDPR (recommendation 20 of this report).

139 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1215 (Taylor Owen).

140 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1220 (Daniel Therrien).

CHAPTER 5: AN INDEPENDENT REGULATOR?

Mr. Therrien told the Committee that any new legislation to regulate privacy on social media platforms should be rights-based and drafted as a statute that confers rights, rather than as an industry code of conduct and should allow for responsible innovation. He recommended that this legislation also "empower a public authority," saying that this could be his office or another public authority to issue binding guidance on how to apply general principles in specific circumstances.[141]

SOCIAL MEDIA PLATFORMS AS BROADCASTERS

During its study, the Committee considered whether social media platforms should be treated the same way as broadcasters.

Michael Pal raised this possibility, saying that if that were the case, when a platform such as Facebook acts like a broadcaster, it would be subject to the same obligations as broadcasters under section 348 of the *Canada Elections Act*, which requires them to charge the lowest available rate to a political party seeking to place an ad on their platform and prevents broadcasters from charging preferential rates to the political parties they prefer.[142] Mr. McKelvey also wondered whether social media platforms should be regulated by the CRTC since, in his view, "they do at times function specifically as broadcasters as well as … a specific new category that deals with this content moderation problem."[143]

Scott Hutton, Executive Director of Broadcasting with the CRTC, confirmed that the organization he works for has some control over broadcasting in Canada and therefore content moderation. The *Broadcasting Act* requires that all broadcasting in Canada be of high standard. With respect to content, the CRTC essentially works in a co-regulatory regime. It enforces a variety of codes that have been developed through public processes with Canadians and with broadcasters to essentially maintain a high standard.

141 Ibid.

142 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1115 (Michael Pal).

143 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1230 (Fenwick McKelvey).

Certain provisions in the CRTC regulations direct how to address matters that contravene the law, that are abusive, or that are false or misleading news.[144]

Mr. Hutton confirmed that the CRTC regulates major broadcasters as well as the "smallest broadcasters [such as] community broadcasters or indigenous broadcasters in rural and remote areas."[145] As a result, a community radio station that can reach a few hundred people is subject to that regulatory oversight, yet a Facebook page that presents content to millions of users is not subject to the same oversight.

As to whether social media platforms, which seem to act more and more like broadcasters of information and news content, should be subject to the *Broadcasting Act*, Mr. Hutton answered yes, stating that "any parties who do benefit from operating broadcasting in Canada should be participating in our system."[146]

Mr. Hutton referred to an interactive report published by the CRTC on 31 May 2018, entitled *Harnessing Change: The Future of Programming Distribution in Canada*, which states that "the traditional regulatory approach is less and less able to obtain the objectives set out in legislation such as the *Broadcasting Act*." The CRTC suggests an innovative approach to policy and regulation for digital platforms guided by three principles, including:

> Secondly, all players that benefit from participation in the broadcasting system should contribute in an appropriate and equitable manner. New policies and regulations must recognize that the social and cultural responsibilities that come with operating in Canada extend to digital platforms.[147]

The CRTC therefore believes that all parties that benefit from operating in Canada should live up to the social responsibilities. That includes social media platforms.[148]

144 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1210 (Scott Hutton, Executive Director, Broadcasting, Canadian Radio-television and Telecommunications Commission).

145 Ibid.

146 Ibid., 1205.

147 Ibid., 1140.

148 Ibid., 1210.

ONLINE CONTENT MODERATION STANDARDS

Mr. McKelvey raised the idea of creating a National Social Media Council, like a broadcasting standards council, "so that you can start coordinating this kind of grey area of content moderation, which is increasingly what platforms do."[149]

He highlighted how this council could be like the CRTC:

> If you look at what the broadcasting standards council looks like, it's very parallel to what has been called for and what we need in content moderation, with an appeals process, transparency, and disclosure. I think the concern and the push-back I have to give back are that's it's more industry self-regulation. I think there is a criticism there, but I think that's an important first step that would actually start convening around this particular activity of content moderation, which we have not recognized well before the law.[150]

The Committee believes that this suggestion is worth considering.

149 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1140 (Fenwick McKelvey).

150 Ibid., 1235.

CHAPTER 6: REGULATION OF THE MONOPOLY POWER OF TECHNOLOGY GIANTS AND DATA-OPOLIES

Since its interim report was published in June 2018, the Committee has been particularly interested in data-opolies held by technology giants and the need to more strictly control their activities. The testimony of Maurice Stucke, the Competition Bureau, the Bank of Canada and the other witnesses cited in this chapter has informed the Committee's thinking in this regard.

RELEVANT EVIDENCE

Maurice Stucke

Maurice Stucke, a law professor with the University of Tennessee's College of Law, appeared before the Committee on 4 October 2018. In March 2018 he published a paper, *Should We Be Concerned About Data-opolies?*[151] which is behind the expression "data-opolies" chosen by the Committee to describe the situation of data monopolies held by a few technology giants.

During his appearance, Mr. Stucke discussed the risks if a few powerful firms monopolize data, in particular how competition officials in the EU and U.S. have viewed them, and the risk of harm that these data-opolies pose to consumers.[152]

Mr. Stucke described data monopolies as follows:

> Data-opolies control a key platform through which a significant volume and variety of personal data flows. The velocity of acquiring and exploiting this personal data can help these companies obtain significant market power.[153]

He then explained the eight potential harms of data-opolies that he has identified:

---

151 Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 19 March 2018, 2 Georgetown Law Technology Review 275 (2018); University of Tennessee Legal Studies Research Paper No. 349.

152 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2018 1110 (Maurice Stucke, Professor, College of Law, University of Tennessee).

153 Ibid.

1) degraded quality
2) surveillance
3) wealth transfer from consumers to data-opolies
4) loss of trust
5) significant costs imposed on third parties
6) less innovation in markets dominated by data-opolies
7) the social and moral concerns of data-opolies
8) the political concerns of data-opolies.[154]

Regarding the fifth harm—significant costs imposed on third parties—Mr. Stucke provided the following clarifications:

> we talk about the frenemy relationship that data-opolies have with app makers. They need these app developers in order to attract users to their platform, but once they start competing with them, they can then have an enemy relationship. There are various anti-competitiveness practices they can engage in, including degrading the app's functionality. What is particularly important for you is that data-opolies can impose costs on companies seeking to protect our privacy interests[155].

For the seventh harm—the social and moral concerns of data-opolies—Mr. Stucke included the concern that data-opolies intentionally make their products addictive:

> Here you have an interesting interplay between monopoly and competition. Ordinarily, a monopolist doesn't have to worry about consumers going elsewhere. Here, however, the data-opolies can profit by getting users addicted to spending more time on their platform. They can thereby obtain more data, target them with advertising and increase their profits.[156]

Lastly, concerning the eighth harm—the political concerns of data-opolies—Mr. Stucke noted that economic power often translates into political power and that data-opolies

154 Ibid.

155 Ibid., 1115.

156 Ibid.

have tools that earlier monopolies did not, "namely, the ability to affect the public debate and our perception of right and wrong."[157]

Mr. Stucke summarized the data-opoly situation in the following three points:

> The first theme is that the potential harms from data-opolies can exceed those from monopolies. They can affect not only our wallets. They can affect our privacy, autonomy, democracy and well-being.
>
> Second, markets dominated by these data-opolies will not necessarily self-correct.
>
> Third, global antitrust enforcement can play a key role, but here, antitrust is a necessary but not sufficient condition in order to spur privacy competition. There really needs to be coordination with the privacy officials and the consumer protection officials.[158]

In answer to questions from the Committee, Mr. Stucke pointed out that in a competitive marketplace, one would think that consumers would get products and services that would be tailored to their privacy interests, but they do not.[159]

He also pointed out that Canadian and U.S. competition officials very much have a price-centric focus on mergers, and increased anti-trust enforcement would improve their tools for non-price effects, including data-driven mergers.[160] According to Mr. Stucke,

> One way would be more informed antitrust enforcement. That's *ex post*. Then you would have, *ex ante*, GDPR-like requirements that could help kick-start privacy. That might be greater data portability so that users can transfer their data. Another might be greater resolution on who owns the data and on the property rights an individual has with regard to personal data.[161]

Regarding data portability – or transferability – Mr. Stucke drew the Committee's attention to the fact that

> there are some measures in the GDPR that look hopeful—such as data portability—and can address some of the competition concerns, but one thing to consider is that data portability may not necessarily be helpful when the velocity of the data is at stake. Here's a good example: mapping apps. You can port your data for Google Maps, let's say, but that's not going to be helpful to a navigation app that needs to know where you are at this very moment. The fact that you can port data from six months ago is not

157 Ibid.

158 Ibid., 1120.

159 Ibid.

160 Ibid., 1125.

161 Ibid.

> going to help that new navigation app compete against Waze, which Google owns, and Google Maps.[162]

When asked to provide recommendations on how to empower the Competition Bureau to handle data-opolies, Mr. Stucke argued that this could be done in part by getting away from price-centric tools when dealing with markets that are ostensibly for free and instead use an alternative such as a small but significant non-transitory decrease in privacy. Mr. Stucke also recommended considering coordination with the privacy authority and the competition authority. In addition, he recommended looking at enforcement actions to ensure that they manage to deter improper behaviour.[163]

Mr. Stucke concluded his appearance by arguing that in order to "get the benefits of a data-driven economy, but in a way so that the economy is inclusive, protects our democracy and also can protect our privacy and improve our well-being," we must get back to the idea that the government has a key role to play in delivering certain essential services that market forces, even in a competitive market, may not provide.[164]

Competition Bureau

The Competition Bureau – under the Commissioner of Competition – is responsible for the administration and enforcement of the *Competition Act* and three other Acts related to labelling.[165] In particular, it is responsible for reviewing merger transactions to ensure that amalgamated corporations do not exercise an inordinate amount of influence over the market to the detriment of customers, suppliers and Canadian consumers, as well as situations involving abuse of a dominant position.

On 19 February 2018, the Competition Bureau released a report entitled *Big data and innovation: key themes for competition policy in Canada*, which is a synthesis of the key themes raised in the context of a public consultation about a Bureau discussion paper ("Big data and Innovation: Implications for competition policy in Canada"). In this report, the Competition Bureau concludes among other things that Canadian competition law in

162 Ibid., 1150.

163 Ibid., 1230.

164 Ibid., 1245.

165 These are: the *Consumer Packaging and Labelling Act*, R.S.C. 1985, c. C-38; the *Textile Labelling Act*, R.S.C. 1985, c. T-10; and the *Precious Metals Marking Act*, R.S.C. 1985, c. P-19.

its current state is adequate for assessing mergers and monopolistic practices in the context of big data.[166]

As for data-driven platforms (the report cites the examples of Google, Uber and Amazon), the Competition Bureau believes that

> The most important insight from platforms is that the nature of a "transaction" or "price" differs from non-platforms. For example, a "high" price on one side of a platform might not be evidence of market power or anti-competitive effects because it results from a "low" price on another side of the platform.[167]

The report also looks at the issue of cartels. On this front, the Competition Bureau argues that the advent of computer algorithms that rely on big data should not lead to a rethinking of competition law enforcement.[168] The Bureau adds that while it is premature to suggest a fundamental change in the enforcement of the provisions of the *Competition Act* related to cartels, it will continue to assess "further evidence on this developing issue."[169]

With regard to advertising, the Competition Bureau notes that its mandate, which involves ensuring truth in advertising, could overlap with that of the OPC, which involves protecting privacy rights.[170] According to the report,

> Both mandates are important to protect consumers in the digital economy. The Bureau will continue to enforce provisions of the Act even if the offending actions may be subject to enforcement under PIPEDA. The Bureau shares the OPC's view of the importance of collaboration in this area and looks forward to working with the OPC to protect Canadian consumers.[171]

The report also refers to the submission filed by the OPC in the context of the Competition Bureau's public consultations. That report states:

> [O]ur Office would be pleased to discuss how the OPC and the Competition Bureau could cooperate in addressing these emerging challenges, in an effort to help business

166 Competition Bureau, *Big data and innovation: key themes for competition policy in Canada*, 19 February 2018, p. 6.

167 Ibid., pp. 6–7.

168 Ibid., p. 9.

169 Ibid., p. 11.

170 Ibid., p. 13.

171 Ibid.

> better understand their compliance obligations to better protect and develop the trust of individuals as it pertains to Canada's digital economy.[172]

In short, the Competition Bureau argues in its report that while the emergence of firms that control and exploit data can raise new challenges for competition law enforcement, that "is not, in and of itself, a cause for concern."[173] The report concludes that while "big data may implicate somewhat specialized and less familiar tools and methods," the traditional framework of competition law enforcement can usefully continue to guide the Bureau's work.[174]

Competition Bureau officials appeared before the Committee on 18 October 2018. Anthony Durocher, the Deputy Commissioner, Monopolistic Practices Directorate, noted two cases where privacy may be relevant to the Competition Bureau's work:

> First, if companies compete to attract users by offering privacy protection, then this dimension of competition can be a relevant factor in reviewing anti-competitive activity. Second, if companies mislead consumers about whether and how their data will be used, this may also raise concerns under the Competition Act.[175]

He also stated the following, with respect to recurring concerns about the size and growth of certain technology companies:

> Becoming big is the reward a firm could get for successfully introducing an innovative product. We should not punish this success. Only when we find evidence that a big firm is engaging in harmful anti-competitive conduct should we intervene.[176]

Regarding competition in the digital economy in general, Mr. Durocher had this to say:

> [I]n the digital economy, we've moved from what we call static competition to dynamic competition. Static competition is this old-world competition on price and output which is still prominent in a lot of industries across Canada. In the digital space, what we're seeing is that companies largely compete for users on the basis of how they're innovating in the offer of their products to consumers. We call this non-price effects.

---

172 Ibid., referring to the 17 November 2017 OPC submission to the Competition Bureau entitled "Consultation on Big Data and Innovation Discussion Paper."

173 Ibid., p. 14.

174 Ibid.

175 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1115 (Anthony Durocher, Deputy Commissioner, Monopolistic Practices Directorate, Competition Bureau).

176 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1120 (Anthony Durocher, Deputy Commissioner, Monopolistic Practices Directorate, Competition Bureau).

> When I talk about modernizing the tools we use for the Competition Act, it's exactly with a view to addressing these issues of non-price effect[177].

Regarding data portability and system interoperability, Mr. Durocher offered the following perspective:

> Data portability of the regulations that we're seeing through the GDPR is the most noteworthy, I think, from a competition perspective. In theory, it can be pro-competitive. It can empower consumers to take their data from one platform to another. Obviously the devil is in the details as to how that's operationalized, but certainly it's something we're taking note of.[178]

Bank of Canada

The Bank of Canada is the country's central bank and its principal role, as defined in the preamble to the *Bank of Canada Act*, is to "promote the economic and financial welfare of Canada." The Bank's four main areas of responsibility are monetary policy, the financial system, currency and funds management.[179]

On 8 February 2018, Carolyn A. Wilkins, Senior Deputy Governor of the Bank of Canada, gave a speech at the G7 Symposium on Innovation and Inclusive Growth ("At the Crossroads: Innovation and Inclusive Growth"). In her speech, Ms. Wilkins discussed the issue of "superstar" firms in the field of information technology – using the examples of social media and online marketplaces – that benefit from market concentration and earn huge monopoly profits. According to Ms. Wilkins,

> What is new is that the "winner-takes-all" effect is magnified in the digital economy because user data have become another source of monopoly power. Data from a large network create a formidable barrier to entry. Another barrier to entry can come from firms using their position as gatekeepers to crucial online services to impede their competitors.[180]

Ms. Wilkins also acknowledged the valuable contribution of the technology sector to economic performance, while noting that the size and market dominance of some firms

177 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1235 (Anthony Durocher, Deputy Commissioner, Monopolistic Practices Directorate, Competition Bureau).

178 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1235 (Anthony Durocher, Deputy Commissioner, Monopolistic Practices Directorate, Competition Bureau).

179 Bank of Canada, *About the Bank*.

180 Bank of Canada, "At the Crossroads: Innovation and Inclusive Growth," p. 4.

raise the usual concerns about the potential effects of monopoly power on prices and competition.[181]

> A new source of market dominance relates to data. Access to and control of user data could make some firms virtually unassailable. They can easily drive out competition by combining their scale with innovative use of data to anticipate and meet evolving customer needs, at a lower price (and sometimes for free). This has a couple of undesirable consequences. First, firms operating in less-competitive environments innovate less; we need the dynamism from firm entry and the contestability of markets to raise the trend line on growth as much as possible. Second, the biggest firms may well return to monopoly pricing in the long run. These consequences get in the way of stronger, more-inclusive growth.[182]

This situation led Ms. Wilkins to recommend prioritizing "the modernization of anti-trust and competition policy, as well as the relevant legal frameworks."[183] In her view, consideration must be given as to how best to remove barriers to entry for new competitors, and how to regulate the ownership and the sharing of user data , given that they "are the primary source of monopoly rents in the digital age."[184] Additionally, Ms. Wilkins mentioned some interesting ideas that have been put forward in this area, such as "giving users control of their data – perhaps even making firms pay users for their data – and regulating tech platforms as utilities."[185]

Ms. Wilkins concluded her speech by arguing that keeping "market power in check, particularly the power that comes from control of consumer data, to encourage competition and limit monopoly profits" is one of three areas (the other two being workforce training and managing operational risk) where a better strategy could be developed and implemented.[186]

A Bank of Canada official appeared before the Committee on 18 October 2018. Eric Santor, the Canadian Economic Analysis Managing Director, expanded on the idea expressed by Ms. Wilkins – in the above-mentioned speech – to the effect that there is the impression that the winner-takes-all effect is magnified in the digital economy because user data has potentially become another source of monopoly:

---

181 Ibid., p. 6.

182 Ibid.

183 Ibid.

184 Ibid.

185 Ibid.

186 Ibid., p. 8.

> Data from a large network creates a formidable barrier to entry in some cases. Another barrier to entry can come from firms using the position as gatekeepers of crucial online services to impede their competitors and thwart innovation. In this context, we believe competition policy can be modernized appropriately to help ensure that benefits of digitalization are fully realized.[187]

As to the issue of superstar firms referred to by Ms. Wilkins in her speech, Mr. Santor said that "one concern in an environment dominated by superstar firms is that those firms have more power when setting prices, which could lead to an increase in prices."[188]

Ben Scott, Tristan Harris and Colin McKay

According to Ben Scott, the time has come to review existing competition policy:

> We need to be looking at modernizing antitrust policy to put shackles on anti-competitive practice, to restrict mergers and acquisitions, and to ease access to market entry for new kinds of services that offer alternatives to the existing models whose externalities have led to such negative outcomes.[189]

Tristan Harris summarized the challenges of competition and system interoperability[190] this way:

> if you were trying to build an alternative to Facebook, YouTube or Twitter, it would be very hard for you to succeed because these are built on network effects.
>
> …
>
> You need to be able to move interoperably between these networks.
>
> …
>
> I think we need to look at similar things like that. What's harder with social networks is that you can't just move my data off to something else because my data is connected to all the posts I've made in other people's profiles and they have privacy settings so that I

187 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1130 (Eric Santor, Managing Director, Canadian Economic Analysis, Bank of Canada).

188 Ibid.

189 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1125 (Ben Scott, Director, Policy and Advocacy, Omidyar Network).

190 Interoperability is "the ability of a computer system, software or interface to work with others, existing or future, without restriction of access or implementation, regardless of the language, location or software involved." See; Laurence Bich-Carrière, "Propriété intellectuelle et émojis : 😉 ou 😱?", in *Développements récents en droit de la propriété intellectuelle*, vol. 449, Éditions Yvon Blais, Montréal, 2018, pp. 314-315 [TRANSLATION].

> can't simply migrate over onto some new platform. I think this is a really important area, and it does have to do with the consolidation of power and the ability for them to quash competition.[191]

Looking at the problem from the other end, Colin McKay mentioned a Google project to facilitate the transfer of data between services. Google developed the project and is now working on it with partners in the industry and, according to a Mr. McKay, it is "a solid attempt to start addressing" the practical problem of system interoperability.[192]

CONCLUSIONS AND RECOMMENDATIONS

In light of the preceding, the Committee believes that in addition to the recommendation it made in its interim report to amend PIPEDA in order to include an obligation to allow data portability, there should also be a recommendation to amend PIPEDA to add the obligation to make systems interoperable so that data could be transferred from one platform to another.

The Committee also believes that the *Competition Act* should be updated to ensure that the Competition Bureau takes non-price effects, such as data-driven mergers, into account in its assessments, and to establish a framework allowing the Competition Bureau and the OPC to collaborate where appropriate. For these reasons, the Committee recommends:

Recommendation 11 on data portability and system interoperability:

That the *Personal Information Protection and Electronic Documents Act* be amended by adding principles of data portability and system interoperability.

Recommendation 12 on modernizing the *Competition Act*:

That the Government of Canada study the potential economic harms caused by so-called "data-opolies" in Canada and determine if modernization of the *Competition Act* is required.

191 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1245 (Tristan Harris, Director, Policy and Advocacy, Omidyar Network).

192 ETHI, *Evidence*, 1st Session, 42nd Parliament, 23 October 2018, 1140 and 1215 (Colin McKay, Head, Public Policy and Government Relations, Google Canada).

Adding to its preliminary recommendation 7 on the sharing of information between the Privacy Commissioner and other regulators (recommendation 25 of this report), the Committee further recommends:

Recommendation 13 on collaboration between the Competition Bureau and the Office of the Privacy Commissioner:

That the *Personal Information Protection and Electronic Documents Act* and the *Competition Act* be amended to establish a framework allowing the Competition Bureau and the Office of the Privacy Commissioner to collaborate where appropriate.

CHAPTER 7: CYBERSECURITY

Since the catalyst of this study was a breach of security of the personal data held by Facebook, the Committee naturally was interested in questions regarding cybersecurity. The testimony given by Communications Security Establishment officials and by Ben Scott, Maurice Stucke, Michael Pal and the Chief Electoral Officer of Canada were particularly valuable in this respect.

RELEVANT EVIDENCE

Communications Security Establishment

According to the Communications Security Establishment (CSE), it is "Canada's centre of excellence for cyber operations."

> As one of Canada's key security and intelligence organizations, CSE protects the computer networks and information of greatest importance to Canada and collects foreign signals intelligence. CSE also provides assistance to federal law enforcement and security organizations in their legally authorized activities, when they may need CSE's unique technical capabilities.[193]

In 2017, in response to a request from the Minister of Democratic Institutions, CSE conducted an assessment of cyber threats to the Canadian democratic process, focusing specifically on federal, provincial, territorial and municipal levels of government with respect to elections, political parties and politicians, and the media. To inform its analysis, CSE examined cyber threat activity against democratic processes in Canada and around the world over the past 10 years. On 16 June 2017, CSE released a report entitled *Cyber Threats To Canada's Democratic Process*, in which it summarized the results of its assessment.

The report recalls, among other things, that there had been a cyber threat against the 2015 federal election in Canada. With respect to the 2019 federal election, CSE expects that "multiple hacktivist groups will very likely deploy cyber capabilities in an attempt to influence the democratic process," and that "much of this activity will be low-

193 Communications Security Establishment, *Cyber Threats to Canada's Democratic Process*, 16 June 2017, p. 3.

sophistication, though we expect that some influence activities will be well-planned and target more than one aspect of the democratic process."[194]

Of note, the CSE report states that "political parties and politicians, and the media are more vulnerable to cyber threats and related influence operations than the election activities themselves."[195] According to the CSE, this is "because federal elections are largely paper-based and Elections Canada has a number of legal, procedural, and information technology measures in place."[196]

The CSE also notes that worldwide, Canada's adversaries[197] use cyber capabilities to target elections, political parties and politicians, and traditional and social media against:

- elections – by suppressing voter turnout, tampering with election results and stealing voter information;
- political parties and politicians – by conducting cyberespionage for the purposes of coercion and manipulation and to publicly discredit individuals; and
- traditional and social media – to spread disinformation and propaganda, and to shape the opinions of voters.[198]

Finally, the CSE believes that "it is highly probable that cyber threat activity against democratic processes worldwide will increase in quantity and sophistication over the next year, and perhaps beyond that." This is because "[m]any effective cyber capabilities are publicly available, cheap, and easy to use" and "[t]he rapid growth of social media, along with the decline in longstanding authoritative sources of information, makes it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media and influence voters."[199]

194 Ibid., p. 4.

195 Ibid., p. 5.

196 Ibid.

197 "Adversaries" are defined on p. 12 of the report as "any states, groups, or individuals who have used or might use cyber capabilities to threaten or influence Canada's democratic process."

198 Communications Security Establishment, *Cyber Threats to Canada's Democratic Process*, 16 June 2017, p. 5.

199 Ibid.

CSE officials appeared before the Committee on 18 October 2018. Dan Rogers, Deputy Chief of SIGINT ("signals intelligence"), told the Committee that CSE had been asked to continue its analysis and expected to release an update to the above-mentioned report.[200]

André Boucher, the Assistant Deputy Minister of Operations, Canadian Centre for Cyber Security, Communications Security Establishment, told the Committee that the update to the report in question is expected in early 2019, and he provided an overview of what to expect:

> Threats have indeed increased, but the main difference is the speed at which threat levels have risen. We were expecting them to rise, but it's happened more quickly. This also applies to Canada. No one will be surprised given what's happening internationally.[201]

Ben Scott's Testimony

Ben Scott also addressed the security issue. In his view:

> This is the simplest and most important piece of the puzzle. The combination of cyber-attack and disinformation campaigns that we have seen unleashed on elections in several different countries is a dire threat, and we have to treat it that way. We need to increase the cybersecurity applied to our democratic institutions, including not just election administration but also political parties and campaigns. They should be treated as critical infrastructure, in my view. We also need to be much better about coordinating the research, monitoring, and exposure of disinformation campaigns that are happening with security services, with outside research entities, and with companies.[202]

Maurice Stucke's Testimony

Mr. Stucke linked the issues of competition and security, making the following observation:

> There are several implications of a security breach or violation of data-opolies' data policies. A data-opoly has greater incentive to protect its data, but hackers also have a greater incentive to tap into this data, because of the vastness that it has. While

200 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1120 (Dan Rogers, Deputy Chief, SIGINT, Communications Security Establishment).

201 ETHI, *Evidence*, 1st Session, 42nd Parliament, 18 October 2018, 1140 (André Boucher, Assistant Deputy Minister, Operations, Canadian Centre for Cyber Security, Communications Security Establishment).

202 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1115 (Ben Scott, Director, Policy and Advocacy, Omidyar Network).

> consumers may be outraged, a dominant firm has less reason to worry about consumers switching to rivals.[203]

Testimony from Michael Pal and the Chief Electoral Officer

On the issue of election cybersecurity, Michael Pal made the following recommendation:

> Cybersecurity costs a lot of money. For example, I think that Canadian banks spend a lot of money trying to ensure cybersecurity. It may be difficult for political parties or entities involved in the electoral sphere. Political parties receive indirect public subsidies through the rebate system, say, for election expenses. One way to incentivize spending on cybersecurity is to have a rebate for political parties or other entities to spend money on cybersecurity.[204]

Mr. Perrault, Chief Electoral Officer, made a similar suggestion:

> the committee may wish to consider the need in the future for parties to receive a special subsidy to help them upgrade and improve the security of their IT systems and explore ways in which such a subsidy could be fairly achieved. I recognize from my own investments at Elections Canada the cost of these investments. I believe it is a matter of public interest, not personal or private interest of the parties, to have the resources as the cost to ensure cybersecurity increases.[205]

Citing what is happening the United States as an example, Mr. Pal also recommended publicizing the protocols on what should happen among government agencies in the event of a cyberattack.[206] He told the Committee that "the public needs to have some confidence about what procedures are followed, because if they don't know what the procedures are, there can be risks that an agency is seen as favouring one side or another, of foreign interference, potentially, on behalf of one party or one set of entities."[207]

---

203 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2018 1110 (Maurice Stucke, Professor, College of Law, University of Tennessee).

204 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1115 (Michael Pal, Associate Professor, Faculty of Law, Common Law Section, University of Ottawa).

205 ETHI, *Evidence*, 1st Session, 42nd Parliament, 1 November 2018, 1135 (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

206 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1120 (Michael Pal, Associate Professor, Faculty of Law, Common Law Section, University of Ottawa).

207 Ibid.

CONCLUSIONS AND RECOMMENDATIONS

In light of the preceding, the Committee finds that political parties would benefit from following CSE's recommendations and that the government would benefit from continuing to study how cyberthreats affect our institutions and our electoral system.

For these reasons, the Committee recommends:

Recommendation 14 on cyberthreats for political parties and the Communications Security Establishment's recommendations:

That political parties follow the recommendations made by Communications Security Establishment that pertain to them regarding electoral cybersecurity.

Recommendation 15 on the need to study cyberthreats:

That the government of Canada continue studying how cyber threats affect institutions and the electoral system in Canada.

CHAPTER 8: RESEARCH, DIGITAL LITERACY AND PUBLIC AWARENESS

LACK OF RESEARCH

Several witnesses were reluctant to make too firm recommendations regarding possible legislative or regulatory measures, noting a lack of information and research on the phenomenon of disinformation and misinformation. For example, Claire Wardle noted that there is only a small body of empirical research on that phenomenon, that she calls information disorders. She noted that:

> The challenges we face are significant and there's a rush to do something right now, but it's an incredibly dangerous situation when we have so little empirical evidence to base any particular interventions on. In order to study the impact of information disorder in a way such that we can really further our knowledge, we need access to data that only the technology companies have.[208]

Ms. Wardle therefore urged governments to pressure social media platforms to allow more research and access to social media platform data, particularly when it comes to elections. Regarding elections, she recommended setting up a specific research unit that can work with the social media platforms to put pressure on them and say, "we need to work with you in a way that we understand who's saying what, and what they do as a result of that." Ms. Wardle believes that we cannot stay stuck in this continuous loop where we keep saying that we need access to data and the platforms say that they cannot provide it because of privacy concerns.[209] She explained:

> I'll go back to my point at the beginning and say that we have so little research on this. We need to be thinking about harm in those ways, but when we're going to start thinking about content, we need to have access to these platforms so we can make sense of it.
>
> Also, as society, we need groups that involve preachers, ethicists, lawyers, activists, researchers and policy-makers, because actually what we're facing is the most difficult question that we've ever faced, and instead we're asking, as Tristan says, young men in Silicon Valley to solve it or—no offence—politicians in separate countries to solve it. The challenge is that it's too complex for any one group to solve.

208 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1105 (Claire Wardle).

209 Ibid., 1250.

> What we're looking at is that this is essentially a brains trust. It's cracking a code. Whatever it is, we're not going to solve this quickly. We shouldn't be regulating quickly, but there's damage.... My worry is that in 20 years' time we'll look back at these kinds of evidence proceedings and say that we were sleepwalking into a car crash. I think we haven't got any sense of the long-term harm.[210]

Mr. Harris also believes that more research is needed into the impact that social media platforms are having on the social fabric. He does not believe that it is the government's role to legislate how technology giants design their products, but they should be held responsible for the externalities that they generate in society (e.g., polarizing harms). In order to hold them responsibility for these externalities, it believes that "we need more research, more funding of that research, to show what those harms are. We need more transparency, because often the only way to know about those harms is to get access to the raw data."[211]

Fenwick McKelvey said that with respect to online advertising, third party data brokers and analytics, and political parties, he hoped that "the committee will also look to new ways to support more research in these areas, giving researchers better access to data under clear ethical guidelines."[212] Ben Scott pointed out that it is important to "be much better about coordinating the research, monitoring, and exposure of disinformation campaigns that are happening with security services, with outside research entities, and with companies."[213] He suggested that the research community needs to be encouraged to spend more time, energy and money on studying the problem since "[w]e simply don't know enough about how disinformation works and how the digital market works to shape political views and electoral outcomes."[214]

DIGITAL LITERACY

In addition to the lack of research, several witnesses agreed that people need to be more educated about the threats posed on various social media platforms and that they need to be taught, for example, how to check the source of the information posted on their newsfeed and how to make sure that the page posting information is run by a human, not a bot.

---

210 Ibid., 1235.

211 Ibid., 1240 (Tristan Harris).

212 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1110 (Fenwick McKelvey).

213 Ibid., 1120 (Ben Scott).

214 Ibid., 1125.

Ben Scott stressed the importance of focusing on the long-term task of addressing public education, stating that people need to be helped to become stronger and more insightful media consumers.[215] He believes that the reason people are vulnerable to misinformation is that he does not have an explanation as to why a social media platform such as Facebook decides to provide him with a particular news item. Unlike the news on CNN or Fox News, there are "10,000 different news items that are sitting in my Facebook account that Facebook could choose to show me, but I'm only going to see about 5% of them. Facebook decides which 5% I'm going to see. It decides that based on what it thinks I want, not what I choose."[216] This makes it important for people to be able to distinguish between legitimate and illegitimate content sources and to be taught some quick and easy ways to evaluate the credibility or the quality of the source.[217]

Elizabeth Dubois said that "we need to ensure that citizens are literate, which includes things like having better informed-consent statements and other media and digital literacy initiatives."[218] She believes that "we need widespread digital literacy programs that really dig into how these digital platforms work so that citizens can be empowered to demand the protection they deserve."[219]

Bianca Wylie said that it was important not to make hasty decisions in the debate on technology and society and to make laws slowly.[220] She gave the example of Sidewalk Labs, a smart city project in Toronto. The project included public consultations, but in an environment, according to Ms. Wylie, where "nobody understands what anybody is truly talking about."[221] She urged the Committee to "consider how much education we need to be doing before we can even be making decisions that are informed by people who live in this country" with respect to technology.[222] She believes that it is important to educate Canadians about what is actually happening right now with their data and privacy.[223]

---

215 Ibid., 1125 and 1130.

216 Ibid., 1130.

217 Ibid., 1140.

218 ETHI, *Evidence*, 1st Session, 42nd Parliament, 2 October 2018, 1105 (Elizabeth Dubois).

219 Ibid.

220 ETHI, *Evidence*, 1st Session, 42nd Parliament, 4 October 2018, 1215 (Bianca Wylie, Co-founder, Tech Reset Canada).

221 Ibid., 1105.

222 Ibid.

223 Ibid., 1215.

Ryan Black also stressed the importance of education, saying that he and his colleague believe that "governments' response must dedicate sufficient resources to education, digital and news literacy and skeptical thinking."[224] He added that he believes public education, such as through an awareness campaign, could be more effective than a legislative tool to regulate social media platforms.[225]

PUBLIC AWARENESS

Mr. Scott said that public awareness requires not only digital literacy but also significant investments in better independent media. He believes that "[w]e can't expect people to steer their way away from nonsense on the Internet if there isn't a large body of quality information and journalism available to them."[226]

Mr. Owen believes that "it's pretty clear that trustworthy information that is known by a large number of citizens is critical to a democracy." Consequently, he thinks that there needs to be a review of how to create more trust and more reliable information in the current ecosystem in the digital public sphere, and that requires reliable journalism.[227]

Mr. McKelvey said that part of the integrity of our democracy is funding public broadcasting.

> [I]n Canada we've kind of said that we have a more proactive cultural policy and that we can function as information subsidies for the public good. When we're talking about trust in the media, this is where public broadcasting has been shown to be really effective in raising the bar for any kind of misinformation or disinformation campaign, making it more difficult to do, and in also putting good information out there. It's really clear to me that the public benefit of public broadcasting is something that is ever more true, that is unique, and it should continue to be part of the robust solution Canada takes to these concerns.[228]

224 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1210 (Ryan Black, Partner, Co-Chair of Information Technology Group, McMillan LLP).

225 Ibid., 1210.

226 ETHI, *Evidence*, 1st Session, 42nd Parliament, 25 September 2018, 1125 and 1130 (Ben Scott).

227 Ibid., 1220 (Taylor Owen).

228 Ibid., 1205 and 1245 (Fenwick McKelvey).

Ms. Wardle also spoke about the importance of supporting quality journalism, offering as an example a project conducted during the recent Brazilian election where 24 major newsrooms worked together to combat disinformation.[229]

The Committee recognizes the need for more research and efforts into digital literacy and public education and therefore recommends:

Recommendation 16 on research regarding online disinformation and misinformation:

That the Government of Canada invest in research regarding the impacts of online disinformation and misinformation.

Recommendation 17 on education and digital literacy:

That the Government of Canada increase its investment in digital literacy initiatives, including for initiatives aimed at informing Canadians of the risks associated with the online prevalence of disinformation and misinformation.

The Committee also wishes to point out that social media platforms, particularly Facebook, which has not been the best corporate citizen in recent years, should also provide time and financial resources to digital literacy initiatives and public awareness. They have immense influence and a significant social responsibility.

As the evidence heard during this study shows, the structural problems that are inherent in social media platforms, which are dependent on the attention economy, result in users constantly consuming information and becoming essentially dependent on the services they offer. Moreover, the powerful algorithms used on these platforms promote content on the basis of principles that are not always pro-democracy, but rather aimed at maximizing advertising revenues or stimulate user interest by manipulating the content they see.

This combination of factors results in the way in which social media platforms operate seemingly contributing in a significant manner to the rapid spread of disinformation and misinformation online. The Committee believes that this reality raises important ethical issues.

These ethical questions will need to be answered if we hope that in the future, giant technology companies will reduce their negative externalities and prevent nefarious actors from using the free tools they provide on their platforms to propagate false,

229 ETHI, *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1240 (Claire Wardle).

divisive or polarizing content, hate speech or any other forms of disinformation and misinformation. In order for Canada to be a leader in this area, the Committee makes the following recommendation:

Recommendation 18 on the addictive nature of some digital products:

That the Government of Canada study the long-term cognitive impacts of digital products offered by social platforms which create dependence and determine if a response is required.

The 18 recommendations made by the Committee above bring nuance or more details to some of the preliminary recommendations contained in its interim report, and include new recommendations on novel concepts studied in the fall. The Committee therefore wishes to reiterate its preliminary recommendations:

Recommendation 19 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**
- **Mandatory registration regarding political advertising outside of Canada.**

Recommendation 20 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.

Recommendation 21 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.

Recommendation 22 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.

Recommendation 23 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.

Recommendation 24 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.

Recommendation 25 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.

Recommendation 26 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

The Privacy Commissioner did not mince his words when describing the current situation: there is a crisis in the collection and processing of online personal data. The Committee does not take such remarks lightly and believes that by sounding the alarm, he has made its recommendations all the more important.

As the Committee concludes this study, it continues to believe that changes to Canada's legislative and regulatory landscape are needed in order to neutralize the threat that disinformation and misinformation campaigns pose to the country's democratic process.

It is critical that the Government of Canada be a leader in bringing in sustainable legislative solutions to protect the personal data of Canadians without hampering innovation. It must also invest the time and resources needed to better educate Canadians about the dangers of the era of disinformation and data-opolies. No effort should be spared so that Canadians can participate in the digital economy and the democratic process without fear.

Lastly, the Committee maintains that if there is one thing that the events of the past year have brought to light, it is that social media platforms should carry out a thorough self-examination, as they have an important choice to make. Do they wish to continue with a business model designed to be addictive while ignoring the harmful effects their platforms can have on the social fabric, and their long-term human impact? Or would they rather make technology more ethical and compatible with the capabilities of the human mind? The Committee sincerely hopes that they will chose the latter.

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

Organizations and Individuals	Date	Meeting
Council of Canadian Innovators	2018/05/10	106
Jim Balsillie, Chair		
Google Canada	2018/05/10	106
Colin McKay, Head, Public Policy and Government Relations		
Office of the Information and Privacy Commissioner for British Columbia	2018/05/10	106
Michael McEvoy, Commissioner		
United Kingdom Information Commissioner's Office	2018/05/10	106
Elizabeth Denham, Information Commissioner		
House of Commons	2018/05/24	108
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		
As an individual	2018/05/29	109
Christopher Wylie		
Office of the Privacy Commissioner of Canada	2018/05/31	110
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		
Daniel Therrien, Privacy Commissioner of Canada		
As an individual	2018/06/07	112
Chris Vickery, Director of Cyber Risk Research UpGuard		
AggregateIQ	2018/06/12	113
Jeff Silvester, Chief Operating Officer		

Organizations and Individuals	Date	Meeting
As individuals	2018/09/25	116
Fenwick McKelvey, Associate Professor Communication Studies, Concordia University		
Taylor Owen, Assistant Professor Digital Media and Global Affairs, University of British Columbia		
Omidyar Network	2018/09/25	116
Ben Scott, Director Policy and Advocacy		
AggregateIQ	2018/09/27	117
Zackary Massingham, Chief Executive Officer		
As individuals	2018/10/02	118
Samantha Bradshaw, Researcher		
Elizabeth Dubois, Assistant Professor Department of Communication, University of Ottawa		
Michael Pal, Associate Professor Faculty of Law, Common Law Section, University of Ottawa		
As an individual	2018/10/04	119
Maurice Stucke, Professor College of Law, University of Tennessee		
Tech Reset Canada	2018/10/04	119
Bianca Wylie, Co-founder		
As individuals	2018/10/16	120
Ryan Black, Partner Co-Chair of Information Technology Group, McMillan LLP		
Vivian Krause, Researcher and Writer		
Pablo Jorge Tseng, Associate McMillan LLP		
Claire Wardle Harvard University		
Centre for Humane Technology	2018/10/16	120
Tristan Harris, Co-Founder and Executive Director		

Organizations and Individuals	Date	Meeting
Bank of Canada	2018/10/18	121
Eric Santor, Managing Director Canadian Economic Analysis		
Communications Security Establishment	2018/10/18	121
André Boucher, Assistant Deputy Minister Operations, Canadian Centre for Cyber Security		
Dan Rogers, Deputy Chief SIGINT		
Competition Bureau	2018/10/18	121
Anthony Durocher, Deputy Commissioner Monopolistic Practices Directorate		
Alexa Gendron-O'Donnell, Associate Deputy Commissioner, Economic Analysis Directorate Competition Promotion Branch		
Google Canada	2018/10/23	122
Colin McKay, Head, Public Policy and Government Relations		
Conservative Party of Canada	2018/10/30	123
Trevor Bailey, Privacy Officer and Director of Membership		
Liberal Party of Canada	2018/10/30	123
Michael Fenrick, Constitutional and Legal Advisor National Board of Directors		
New Democratic Party	2018/10/30	123
Jesse Calvert, Director of Operations		
Canadian Radio-television and Telecommunications Commission	2018/11/01	124
Neil Barratt, Director Electronic Commerce Enforcement		
Rachelle Frenette, Legal Counsel		
Scott Hutton, Executive Director Broadcasting		

Organizations and Individuals	Date	Meeting
Elections Canada	2018/11/01	124
Anne Lawson, Deputy Chief Electoral Officer Regulatory Affairs		
Stéphane Perrault, Chief Electoral Officer		
Office of the Privacy Commissioner of Canada	2018/11/01	124
Julia Barss, General Counsel and Head of Legal Services Legal Services Directorate		
Brent Homan, Deputy Commissioner Compliance Sector		
Gregory Smolynec, Deputy Commissioner Policy and Promotion Sector		
Daniel Therrien, Privacy Commissioner of Canada		

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.

Eatz, Sydney

Oath Inc.

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. 99 to 102, 104, 106, 108 to 114, 116 to 124 and 127 to 129) is tabled.

Respectfully submitted,

Bob Zimmer
Chair