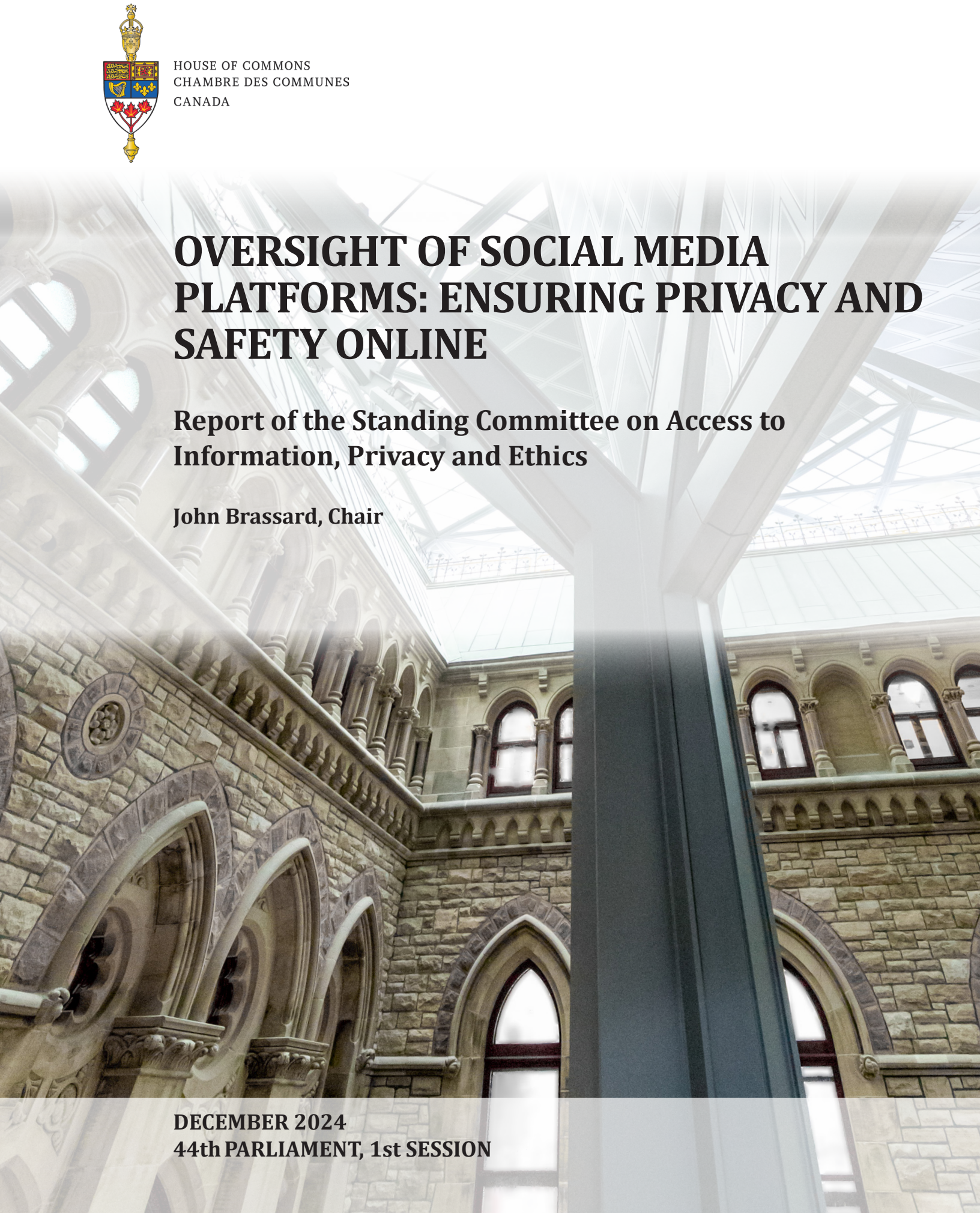

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

OVERSIGHT OF SOCIAL MEDIA PLATFORMS: ENSURING PRIVACY AND SAFETY ONLINE

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

John Brassard, Chair

DECEMBER 2024
44th PARLIAMENT, 1st SESSION

OVERSIGHT OF SOCIAL MEDIA PLATFORMS: ENSURING PRIVACY AND SAFETY ONLINE

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

John Brassard
Chair

DECEMBER 2024

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees 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

John Brassard

VICE-CHAIRS

Darren Fisher

René Villemure

MEMBERS

Parm Bains

Michael Barrett

Frank Caputo

Michael Cooper

Matthew Green

Anthony Housefather

Iqra Khalid

Brenda Shanahan

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Hon. Carolyn Bennett

Maxime Blanchette-Joncas

Alexandre Boulerice

Larry Brock

Pam Damoff

Eric Duncan

Ali Ehsassi

Nathaniel Erskine-Smith

Damien C. Kurek

Hon. Mona Fortier

Marilyn Gladu

Jacques Gourde

Lisa Hepfner
Mike Kelloway
Viviane Lapointe
Bryan May
Glen Motz
Kyle Seeback
Francesco Sorbara
Karen Vecchio

CLERK OF THE COMMITTEE

Nancy Vohl

LIBRARY OF PARLIAMENT

Research and Education

Alexandra Savoie, Analyst
Maxime-Olivier Thibodeau, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

SIXTEENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(h), the committee has studied the use of social media platforms for data harvesting and unethical or iIllicit sharing of personal information with foreign entities and has agreed to report the following:

TABLE OF CONTENTS

SUMMARY

Social media platforms have been part of the information ecosystem for several years now. A large percentage of Canadians, including children and teenagers, use these platforms and share willingly their personal information online.

This report tackles an important issue: how can we exercise better oversight of social media platforms to ensure that the information Canadians provide to these platforms is protected and used appropriately, as well as ensure online safety for everyone?

The report provides an overview of social media platform practices, exploring such aspects as their business models and the way they collect, use and share personal information, especially when it comes to minors. It highlights the contrast between how academic, experts and social media platform representatives describe and evaluate these practices. The report also discusses what these platforms do to protect the data they collect, respond to external threats and counter attempts at foreign interference.

There is also a particular focus on TikTok, the social media platform explicitly mentioned in the motion that led to the Committee's study. For example, the Committee was interested in the ban on the use of this app on Government of Canada devices.

Lastly, the report outlines the measures, legislative and other, proposed by the witnesses to ensure better oversight of social media platforms. It also discusses education and awareness, two aspects seen by several witnesses as crucial in the fight against bad actors using social media platforms for nefarious purposes.

In light of the evidence heard, the brief it received and additional documentation provided by certain witnesses, the Committee makes 8 recommendations.

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.

OVERSIGHT OF SOCIAL MEDIA PLATFORMS: ENSURING PRIVACY AND SAFETY ONLINE

INTRODUCTION

On 31 January 2023, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the Committee) adopted the following motion:

> That, pursuant to Standing Order 108(3)(h), the committee undertake a study of the use of social media platforms such as TikTok and its parent company, ByteDance Ltd., but not limited to, and their involvement or use of private information of Canadians for the objective of data harvesting and unethical/illicit sharing of personal information with foreign entities; that the committee study whether this private data and information of Canadians is adequately protected and stored; that the committee invite relevant witnesses from: the Canadian Communications Security Establishment, key executives from ByteDance Ltd., relevant cybersecurity experts and watchdogs to testify; that the Committee devote a minimum of three meetings with witnesses to this study; and that the committee report its findings to the House.

Interpreting this motion broadly, the Committee was also interested in other aspects of social media platforms, such as their business model, privacy practices—especially those concerning minors—and content moderation. The study resulting from this motion took place between 18 October and 13 December 2023. The Committee held 6 public meetings, heard 24 witnesses and received 1 brief.

The report is divided into four chapters. Chapter 1 deals mainly with social media platform practices, as described by experts and academics, as well as by platform representatives. Chapter 2 discusses the potential sharing of personal information collected by social media platforms with foreign actors. Chapter 3 focuses on legislative, regulatory and other measures that would enable Canada to ensure better oversight of social media platforms. Lastly, Chapter 4 deals with education and awareness. The Committee's recommendations are presented in the relevant chapters.

CHAPTER 1: SOCIAL MEDIA PLATFORM PRACTICES AND RELATED ISSUES

Overview of practices

As explained by Brett Caraway, Associate Professor of Media Economics at the University of Toronto, a lot of data is harvested by the most prominent social companies, such as Facebook, Google, Instagram and TikTok. They collect all their users' personal data and also track all their transactional and interaction data. He explained, for instance, that Facebook is successful because it is able to leverage its users' social connections at scale, and Google is successful because it can leverage its users' purchasing intent at scale.

Mr. Caraway stated that too often there are divergences between public and private interests in the digital platforms market. He explained that users, advertisers and platform operators each have their own set of incentives. He gave the example of Instagram, which has a financial incentive to maximize the number of users and their level of engagement, thus making the platform more attractive to advertisers. He said that advertisers want as much information as possible about the platform's users so they can minimize uncertainty. Users, on the other hand, just want to enjoy the functionality of the platform with as little disruption as possible.

Mr. Caraway explained that every time a user enters a search query on Google, watches a video on TikTok, likes someone's post on Facebook or retweets something on X, information is gathered, auctions take place and commercial messages are delivered. He shared his concerns about the adverse impacts that these platforms are having on the public sphere, even when they work exactly as intended. He added that the platforms' business model all but guarantees the propagation of disinformation, efforts to influence behaviour and the erosion of individual privacy.

Along those lines, Anatoliy Gruzd, Professor and Canada Research Chair in Privacy-Preserving Digital Technologies, Toronto Metropolitan University, said that users who share personal information on social media platforms or a website are tracked, which he thinks is a pervasive practice across the board and across the industry.

Regarding the risks arising from the use of social media platforms, Emily Laidlaw, Associate Professor and Canada Research Chair in Cybersecurity Law, University of Calgary, argued that privacy is just one part of the equation. She gave the example of Discord, a platform that does not use tools to detect child sexual abuse content, monitor livestreamed content or offer a tool for reporting problematic content. In her view, this illustrates a safety design problem on top of a privacy problem. Unfortunately, many

popular platforms only do the bare minimum to govern the risks of their products, according to Dr. Laidlaw.

Echoing some of the comments made by other witnesses, Joe Masoodi, Senior Policy Analyst with The Dais, a public policy and leadership institute at Toronto Metropolitan University, said that social media platforms collect, transfer and store a wide variety of personal and sensitive information, including personal identifying information, private messages, and location, financial information and biometric data.

Mr. Masoodi believes that social media platforms have been designed to keep individuals online and engaged to reap as much data about them as possible. The platforms then aggregate this data to create detailed profiles and inferences about individuals, including their political opinions, sexual orientation, religion, income, health, or details about their families. Mr. Masoodi argued that this describes TikTok's practices, but this also applies to most major online platforms.

Mr. Masoodi is also of the view that there are currently inadequate protections over how Canadians' personal data is transferred and stored, particularly outside of Canada, despite the significant risks through the potential misuse of this data. He argued that this lack of protection threatens Canadian sovereignty and the digital security and privacy of Canadians.

Among the risks raised by Mr. Masoodi is access to personal data by national security and law enforcement agencies in certain countries without sufficient legal protections, such as China.[1] In addition to that risk, technology companies can also experience buyouts, mergers or bankruptcy that could change where and how personal data is stored and privacy protections offered by those companies. Mr. Masoodi believes that malicious actors could also take advantage of data with insufficient safeguards.

On the topic of cross-border transfers of data, Sam Andrey, Managing Director of The Dais, mentioned a report entitled *Home Ice Advantage*, co-written with Mr. Masoodi and their former colleague Yuan Stevens, that examines the transborder data security of

1 Another example is the ability for law enforcement agencies, under the United States *Foreign Intelligence Surveillance Act*, to compel a communications service provider, subject to U.S. law, to turn over data under its control. See : Stevens, Y., Masoodi, M.J. & Andrey, S, *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*, Cybersecure Policy Exchange, 2020, p. 13. With respect to foreign cyberthreats, as indicated later in this report, witnesses identified countries other than China that conduct such activities, including Russia, Iran, North Korea and Mexico.

social media platforms. Measures to better regulate cross-border data transfers are further discussed in Chapter 3 of this report.[2]

This overview offers a glimpse into the many issues raised by witnesses with respect to the way in which social media platforms operate, collect, use, store and share data, which can impact users of these platforms. This chapter provides more details on the practices of social media platforms. The evidence heard by the Committee makes apparent the contrast between how academics and stakeholders evaluate these practices, and how the platforms assess their own practices.

A Business Model Based on Advertising Revenues and the Attention Economy

Philippe Dufresne, Privacy Commissioner of Canada, referred to the expression "if it's free, you're the product" to illustrate how important it is that Canadians understand that, even if they feel they are receiving a free product or service, they are giving up a fundamental part of their identity to companies that collect their personal information. Similarly, Mr. Caraway pointed out that, even though some services appear to be free, in an advertising-supported model, users are paying for that when they purchase goods or services later on. Dr. Gruzd made similar comments.

Mr. Caraway said that the business model drives advertisers to demand more and more data, so platform operators harvest more and more. In fact, according to him, in the platform business model, there is no effective upper limit to the exploitation of human attention. He said that the economic function of advertising is to capture our attention, which is scarce by nature, away from its competing uses. Mr. Caraway argued that how we choose to allocate our attention is important, both for individuals and for society: "our attention shapes who we are, who we might be and where we might go."

Dr. Laidlaw told the Committee that much of the transparency seen from companies is actually more of a marketing exercise than them being upfront about what some of their practices are, specifically when it comes to advertising that targets children.

Data Collection, Use and Sharing

Sharon Polsky, President of the Privacy and Access Council of Canada, said that many companies scrape data that they consider public because they find it online. She

2 Stevens, Y., Masoodi, M.J. & Andrey, S, *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*, Cybersecure Policy Exchange, 2020.

believes it is too easy for any organization to use personal information that has been amassed online to sway views of public policy, government, legislators, teachers and institutions. In her view, this is a threat to democracy, civil liberties and human rights.

As to whether social media companies know that their data is being misappropriated or that they are allowing their data to be misused by third parties, Dr. Laidlaw stated that it is a bit of both: these companies are not providing the full picture, but they also do not fully know what is happening either. She stated that there are various apps that say they have all the child protection measures available, but in practice, do not. She did not specify which apps she was referring to.

Explicit Content and Child Exploitation

Some members also raised questions about to the propagation of sexually explicit content online. Jeanette Patell, Head of Canada Government Affairs and Public Policy for Google and YouTube, and Rachel Curran, Head of Public Policy for Canada at Meta Platforms Inc. (Meta), said that pornography and sexually explicit content are prohibited on YouTube and Facebook. Wifredo Fernández, Head of Government Affairs, United States of America and Canada at X Corporation (X), explained that users who are under 18 or who did not include a birthdate on their profile are restricted from viewing explicit content on X.

The Google and Meta representatives also told the Committee how sexually explicit content is removed from their platforms and how the reasons for content removal are released. For example, according to Google, as Ms. Patell explained, over 90% of the time, prohibited content is first detected by machines, allowing Google to deal with this at scale and to do it rapidly.

Ms. Curran said that restrictions on the display of sexual activity also apply to digitally created content unless it is posted for educational or satirical purposes.

Mr. Fernández said that X restricted the search for this kind of material over the last year, increased training for agents to make reports to the cyber tip line, and automated its process for reporting to the cyber tip line for the National Center for Missing & Exploited Children (NCMEC) in the United States, which acts as a global clearing house for tip lines in different jurisdictions.

On that point, Ms. Patell told the Committee that Google and YouTube provide hashes of child sexual exploitation content to NCMEC and to other platforms so that this content

cannot be recirculated elsewhere. Ms. Curran added that Meta supports the development of a case management tool for NCMEC cyber tips.

Mr. Fernández added that X recently announced a product partnership with Thorn, an organization fighting the sexual exploitation of children, to enhance its capability of detecting sexually explicit content online. As for Meta, Ms. Curran said that it has built partnerships with other anti-trafficking experts and child safety organizations like OneChild in Canada, Polaris and Stop the Traffik, in addition to Thorn.

Ms. Curran also said that Meta has developed new technologies to prevent its platforms from being used for the sexual exploitation of children. She stated that Meta has removed more than 34 million pieces of child exploitation content from Facebook and Instagram in the fourth quarter of 2022 and that over 98% of that was detected before it was reported. To detect and prevent child grooming or potentially inappropriate interactions between minors and adults, Meta uses a combination of technology and behaviour signals.[3]

The Committee notes that despite efforts outlined by the representatives of social media platforms, sexually explicit content, including some relating to children, appear to clearly remain present on these platforms. In January 2024, for example, the chief executive officers of the five major social media companies, Meta, Snap, Discord, TikTok, and X, appeared before the U.S. Senate Judiciary Committee to discuss the availability of harmful content available to children on these platforms, including child sexual abuse material.[4]

On the law enforcement side, Bryan Larkin, Deputy Commissioner, Specialized Policing Services at the Royal Canadian Mounted Police (RCMP), told the Committee that the RCMP has ongoing relationships with all social media platforms through the National Cybercrime Coordination Centre. The RCMP also has protocols in place, particularly around child exploitation and harm to young people.

Legitimate Government Requests for "Lawful Access" and to Take Down Content

Google, Meta and X explained the process they use to evaluate legitimate requests for "lawful access" to user information or to take down content from various governments

3 House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Evidence*, Rachel Curran (Head of Public Policy, Canada, Meta Platforms Inc.).

4 United States, Senate Committee on the Judiciary, *Protecting Children Online*.

based on U.S. law, local laws and international standards, such as the Global Network Initiative's Freedom of Expression and Privacy Principles,[5] and how they publish this information in transparency reports or on their website. TikTok provided a similar explanation in their written response.[6]

Ms. Patell added that if the relevant Google team believes that a request is asking for too much information, they will try to narrow it, and in some cases, object to producing any information at all. Similarly, Nathaniel Gleicher, Head of Security Policy with Meta, said that Meta pushes back on requests it deems to be overly broad.

In a written response to questions put to Google by Committee members during their appearance, Google also mentioned that sometimes it receives requests for information in emergencies, such as bomb threats, school shootings, kidnappings, suicide prevention and missing person cases. In such situations, Google stated that it may provide information to a government agency, as long as it would prevent someone from dying or from suffering serious physical harm.[7]

Mr. Fernández said that law enforcement agencies have a special portal where they can make lawful requests for data on X users or for content removal.

With respect to taking down content, Steve de Eyre, TikTok's Director of Public Policy and Government Affairs for Canada, said that TikTok's policies and community guidelines posted on their website outline what is not allowed on the platform. A team of over 40,000 safety professionals work every day to moderate content and take down anything that violates TikTok's guidelines. Content moderators are around the world, including in Canada. He said that a user can report a video that violates TikTok's guidelines and the company will remove it.

For example, Mr. de Eyre said that in the second quarter of 2023, TikTok removed 885 videos, or less than 1% of all videos uploaded in Canada, with 90% of those videos removed proactively, without any user reporting the content.[8]

As for law enforcement, Mr. Larkin said that the RCMP follows up on legitimate requests for access to social media users' personal information, production orders and search

5 Google Canada, *Written response submitted to ETHI*, p. 2 [HYPERLINK NOT AVAILABLE].

6 TikTok, *Written response submitted to ETHI*, p. 2 [HYPERLINK NOT AVAILABLE].

7 Google Canada, *Written response submitted to ETHI*, p. 2 [HYPERLINK NOT AVAILABLE].

8 Tik Tok, *Content violations and bans*. TikTok indicates that it uses automated and human evaluation to detect and take action against violations or its community guidelines and remove content.

warrants to obtain further information from social media platforms. He noted that the RCMP has ongoing protocols with the security departments of these platforms to receive and retrieve the requested information, which then becomes evidence in an investigation.

Use of Artificial Intelligence for Foreign Interference or Disinformation Purposes

Lindsay Hundley, Influence Operations Policy Lead at Meta, said that foreign interference operations using content generated by artificial intelligence (AI) is not new: Meta has detected coordinated inauthentic behaviour (CIB) on its platforms starting in 2019. She explained that Meta uses behaviour-based detections of AI-generated content and that over two-thirds of CIB operations removed by Meta in 2022 featured this type of content.

Dr. Hundley added that Meta has seen newer operations using the latest generative AI techniques, which will pose future challenges. She said Meta's experience has shown that a behaviour-based approach is still well suited for identifying covert influence operations early in their life cycle because these operations leave a lot of behavioural signals by posting this kind of content that Meta can still detect.

Samy Khoury, Head of the Canadian Centre for Cyber Security (CCCS), which is affiliated with the Communications Security Establishment (CSE), said the CCCS is concerned about the misuse of AI, such as when it is used to amplify misinformation with the use of bot farms, for example. The CCCS is also concerned about information leakage through AI during online interactions. That is why it provides advice and guidance to Canadians on how to use existing AI tools and how some countries or some states are trying to exploit algorithms for their own benefit.

For example, Mr. Khoury said that the CCCS conducts research on the state of the art of AI, gives presentations and publishes articles. It also works closely with CSE so it can provide guidance to government departments on how to use AI.

Dr. Hundley offered an example of how AI can be used for an influence operation. She told the Committee how Meta detected and removed a cluster of commenting activities from the influence operation known as "spamouflage" that targeted, among others, audiences in Canada. She said that spamouflage is a long-running, cross-Internet operation with global targeting, and that Meta and other industry peers have been countering it since 2019. She also noted that in August 2023, Meta removed thousands of accounts and pages after it connected different clusters of activities together to be

part of a single operation attributed to individuals associated with Chinese law enforcement.

According to Dr. Hundley, this particular activity, known as spamouflage, is a cross-Internet operation, traces of which were found on over 50 platforms and forums across the Internet, including Facebook, Instagram, X, YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, Vimeo and dozens of other smaller platforms. In her view, this shows that countering foreign interference is something that requires a whole-of-society effort.

Google is also tracking "Spamouflage Dragon," also known as "Dragonbridge," said Shane Huntley, Senior Director of the Threat Analysis Group. However, Dr. Hundley and Mr. Huntley noted that despite their scale, these campaigns do not necessarily have any real harmful impacts. This type of operation often ends up with zero engagement with real users.

Use of artificial intelligence by law enforcement

In a written response to questions put by Committee members to RCMP officials during their appearance, the RCMP wrote that from a law enforcement perspective, the RCMP sees AI "as a dual use technology, one that can aid law enforcement, especially in data rich and complex investigations, but can also be used by criminal threat actors in Canada to victimize Canadians and affect Canada's interests."[9]

According to the RCMP, AI could have significant impacts for Canada in its efforts to counter foreign interference as it is a force multiplier for disinformation and enables the creation of deepfakes, all of which will increasingly surpass human capacity for detection.[10] The RCMP's written response states the following:

> The RCMP is assessing the threat of criminal use of AI as a factor in across a spectrum of criminal activity, from fraud to foreign interference. The rapid development and ease of access to AI based technology by criminal threat actors is a known area of concern. The use of generative AI for the creation, amplification, and dissemination of disinformation/misinformation will likely be used to sow distrust of Western institutions. The ease of creation and possible prolific dissemination will likely far outpace counter narratives from official channels.[11]

9 Royal Canadian Mounted Police, *Written response submitted to ETHI*, p. 1 [HYPERLINK NOT AVAILABLE].

10 Ibid.

11 Ibid.

In its written response, the RCMP goes on to say that it is equipped with technology that can be of assistance to any investigation into offences where AI is alleged to have been used for nefarious purposes, including deepfakes, and in any context, including foreign interference.

Foreign Interference and Elections

When it comes to elections, Mr. Khoury told the Committee that the role of the CCCS is to collaborate with Elections Canada to ensure that elections infrastructure is properly protected, which it did during the most recent federal election. He added that this role does not include checking online content, as the CCCS mandate is rather to protect infrastructure security.

Brigitte Gauvin, Acting RCMP Assistant Commissioner, Federal Policing, National Security, said that the RCMP has a shared mandate with the Office of the Commissioner of Canada Elections concerning allegations of foreign interference during elections. She said that the RCMP has a variety of ways to warn targeted individuals.

On this point, Mr. Fernández referred to X's civic integrity policy, which targets four areas of potential violations: misleading information that could deceive voters about how to participate in an election, misleading information that could intimidate people from participating, information that could suppress the vote, and impersonation. Mr. Fernández also referred to "Community Notes," a feature that allows X users to add context to content that they believe may be misleading in order to help other readers.

According to Mr. de Eyre, TikTok partnered with Elections Canada to build a bilingual, in-app election centre that provided authoritative information to Canadians, such as where to vote. He also said that TikTok signed on to the Canada Declaration on Electoral Integrity Online.

Questions relating to social media platforms and foreign actors are more broadly discussed in Chapter 2. The next four sections contain evidence provided by the four social media platform representatives who have appeared before the Committee on their practices. As already indicated in chapter 1, and as will be evident in chapter 3, when discussing legislative and other measures that could be adopted to better protect privacy and safety online, many witnesses would likely not agree with certain statements made by platform representatives regarding their practices, including the idea that they do not collect excessive data.

TikTok's Practices: the platforms' position

Mr. de Eyre told the Committee that millions of Canadians and over a billion people around the world use TikTok.

This statistic appears to be confirmed by the latest Social Media Lab report on the state of social media, which indicates that most of the top nine platforms used by Canadians are North American and U.S.-based, and that TikTok is the fastest-growing platform.[12]

Data Collection and Use by TikTok

According to Mr. de Eyre, TikTok collects information that users choose to provide. Information collected by TikTok include:

- phone number or email (e.g., to register an account);
- birthdate (e.g., to provide the user with an age-appropriate experience);
- payment information for accounts that use paid features (e.g., virtual gifting);
- likes, shares, and browsing history in order to recommend more relevant content;
- device Information, including information about the device used, such as its model, operating system and settings such as time zone and language, in order to perform a number of security functions (e.g., mitigating spam) and to allow advertisers to optimize and measure the effectiveness of their ad campaigns; and
- approximate location to show relevant content and ads based on the region a user is in.[13]

In a written response to questions put by Committee members during their appearance, TikTok representatives also confirmed that it collects the IP addresses of its users. It also

12 ETHI, *Evidence*, Anotoliy Gruzd (Professor and Canada Research Chair in Privacy-Preserving Digital Technologies, Toronto Metropolitan University); Philip Mai and Anatoliy Gruzd, *The State of Social Media in Canada 2022*, Social Media Lab, Toronto Metropolitan University, September 2022.

13 TikTok, *Written response submitted to ETHI*, p. 1 and pp. 5–6 [HYPERLINK NOT AVAILABLE]. TikTok, *Privacy Policy*. A more detailed description of all the types of information that are collected by TikTok is found in the privacy policy.

states that TikTok treats anyone who visits its platform, whether or not they logged in with an account, as a user. TikTok says that it collects certain technical information from users not logged in with a TikTok account, such as the device language setting and IP address.[14]

This was confirmed by Dr. Gruzd. He told the Committee that soon after installing the TikTok app on his phone, even without creating an account, he began receiving requests for information from the app such as his battery life and device ID.

On the issue of user location, David Lieber, Head of Privacy Public Policy for the Americas at TikTok, told the Committee that the company does not collect precise location information, but rather users' approximate location, based on the IP address, such as to identify the province or city where the user is.

TikTok representatives also said that while it does collect the content of messages on its platform to power the direct messaging function, it does not collect messages from other apps.

> We may access in-app direct messaging content, for example, to promote the safety and security of the platform, which may include reviewing such content and metadata for violations of our Terms of Service, Community Guidelines, or threats to the safety and security of our community and the broader public.[15]

According to representatives, TikTok does not engage in aggressive data harvesting. It collects information that its users choose to provide and information that helps the app function, operate safely and improve user experience.

Regarding the collection of biometric data by TikTok, Mr. Lieber confirmed that it does not use such data to identify users. TikTok representatives confirmed that it does not collect or use biometrics to "infer" user characteristics such as age, gender or interests. However, it does use face and voice information for various non-identifying purposes, such as when a user opts to use a visual effect or filter.[16]

14 TikTok, *Written response submitted to ETHI*, p. 2 [HYPERLINK NOT AVAILABLE].

15 Ibid., p. 6.

16 Ibid.

In their written response, TikTok representatives also explained that it does not identify individuals or infer sensitive information based on what a user watches on their platform.[17] Here is Mr. de Eyre's explanation of how the TikTok algorithm works:

> Essentially, the way the TikTok algorithm works is that it looks at signals on how you interact with videos. There are positive signals: Do you like it, comment on it or share it? Do you watch the whole video? Do you watch it again? There are also negative signals: Do you swipe away from it within a couple of seconds? Based on that, we can identify what types of videos you like and look at similar other users who have interacted similarly with that video and then recommend additional content to you. That really allows Canadians to find content and to be recommended content that they think they're going to love.[18]

In its written response, TikTok explained that content is recommended by ranking videos based on a combination of factors centred around a user's activity. The "Why this video" feature provides more information about why a particular video appeared in a user's "For You" feed.[19]

TikTok users can also influence the content that they see, such as by using the "Not interested" feature to see less of a certain type of content. A new tool also filters out videos with keywords and hashtags that a user may not want to see in their "For You" feed. This feature is included in its "Family Pairing" set of tools, TikTok's parental control feature.[20]

With regard to minors, Mr. de Eyre said that TikTok has built policies based on leading research by not-for-profit agencies on the experience of youth online in order to provide them with an age-appropriate experience. For example, age-appropriate content labelling was introduced into the system so that some types of videos are labelled and will not be recommended to a user who is under 18. When recommending content to users, TikTok also collects information about what a user views and the length of time the user spends watching the video, as this is an important factor in determining whether content is relevant and interesting to a particular user.[21]

---

17 Ibid., p. 3.

18 See also: ETHI, *Evidence*, Steve de Eyre (Director, Public Policy and Government Affairs, Canada, TikTok).

19 TikTok, *Written response submitted to ETHI*, p. 5 [HYPERLINK NOT AVAILABLE].

20 Ibid.

21 Ibid., p. 6.

Sharing and Storage of Data Collected by TikTok

Mr. Lieber confirmed that data collected by TikTok is stored on its servers in the U.S., Singapore and Malaysia. Mr. de Eyre said that TikTok's operations in Canada are subject to Canadian privacy law, despite the fact that the data is stored abroad.

On this point, Mr. Dufresne said that Canadian privacy legislation will still apply if Canadians are affected. A number of factors give the Office of the Privacy Commissioner (OPC) jurisdiction, even if the information itself is stored elsewhere. When there is a sufficient connection, the legislation applies to the processing of personal information.[22]

Referring to Mr. Lieber's testimony about where TikTok's servers are located, Mr. Andrey, however, argued that this does not provide the complete picture because TikTok's servers can be accessed remotely from any country in the world.

Matt Malone, Assistant Professor, Faculty of Law, Thompson Rivers University, told the Committee that according to Chinese law, specifically the National Intelligence Law, companies operating in China are required to co-operate with China. One provision of this law also calls for its extraterritorial application. Mr. Malone said the fact that the Chinese state holds a 1% share in TikTok and ByteDance allows it to control these companies, meaning that the problems surrounding the transfer of data are not going to go away. The concerns over company control are explored further in Chapter 2.

Regarding data sharing, Mr. Lieber said that some can be shared with TikTok's advertising partners. Mobile identifiers help match up a TikTok user and an action they may have taken on an advertiser's website. He said that these partners have access just for the purpose of understanding, for example, how their TikTok advertising campaigns worked and to obtain statistics such as how many people looked at an ad.

With regard to the sharing of data with ByteDance, TikTok noted that personal information from Canadian users is collected in accordance with the company's privacy policy. Some ByteDance entities provide services that support the operation of the TikTok platform and are therefore given remote access to Canadian user data. TikTok representatives said that a series of robust controls, safeguards like encryption, and a

22 See: *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII). The Federal Court ruled that the *Personal Information Protection and Electronic Documents Act* has extraterritorial application because of the existence of a real, substantial connection with Canada.

multi-step approval process based on the principles of need to know and least privilege help ensure that data is only accessed by those who really need it.[23]

Mr. Lieber explained that in fact, TikTok operates by the principle of least privilege, meaning that any employee looking to access user data must make a request and obtain approval following a rigorous review. He added that TikTok has data classification policies with increasing levels of sensitivity of data, with user data being the most sensitive.

Data Security

On the topic of the security of Canadian users' data, Mr. Lieber said that TikTok has a privacy policy, that it publishes information about the data it collects, how it is used, the extent to which it may be disclosed and under what conditions. He said that TikTok also provides extensive settings that its users can utilize to protect their data. TikTok also noted that it has the ISO 27001 certification, which is one of the most globally recognized information security standards in several countries, including the U.S.[24]

In its written response, TikTok also said that it maintains a rigorous third-party management program to ensure that its partners uphold the same security standards as it does.[25] TikTok also explained that, like other platforms, its privacy policy states that it cannot guarantee the security of information transmitted via the platform.

Practices Concerning Minors

Mr. de Eyre told the Committee that TikTok has developed measures to protect teens, such as limiting the age at which someone can create an account. Mr. Lieber said that one age-gating function used by TikTok to prevent individuals under 13 from opening an account is that it does not provide any clues as to the eligibility age, meaning that new users do not know that by providing their age, they are indicating to TikTok whether they are old enough to open an account.

Mr. Lieber said that during the second quarter of 2023, TikTok removed over 18 million accounts globally of users who were suspected of being under 13.

---

23 TikTok, *Written response submitted to ETHI*, pp. 1–2 [HYPERLINK NOT AVAILABLE].

24 International Organization for Standardization, ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection, Information security management systems, Requirements.

25 TikTok, *Written response submitted to ETHI*, p. 2 [HYPERLINK NOT AVAILABLE].

In its written response, TikTok says that its platform is for users 13 and over (14 and over in Quebec), that it provides age-appropriate privacy settings and controls and has built-in protections by default. For example, accounts of those aged 13 to 15 are private by default. Direct messaging is disabled for users under 16. The accounts of users under 18 years of age cannot use the livestreaming feature, and every account belonging to a user below age 18 is set to a 60-minute daily screen time limit by default.[26]

However, these settings can simply be changed, as Mr. Caraway told the Committee, and a user can continue using the app by entering a passcode once 60 minutes have elapsed.

TikTok referred to other safeguards, such as parental control, which can be activated by linking a parent's TikTok account to their teen's. This includes screen time management, push notification scheduling and limiting content from appearing in the child's feed that may not be age appropriate.[27]

Regarding youth education, Mr. de Eyre said that TikTok has partnered with Canadian not-for-profit organizations such as MediaSmarts, Kids Help Phone, Tel-jeunes and Digital Moment to support their work to educate Canadians and to create resources for online safety, well-being and digital literacy.[28]

In its written response, TikTok says that searches for certain hashtags are redirected to support resources, while harmful hashtags are blocked.[29]

As for educating teens about the data they share, Mr. de Eyre reiterated that TikTok has several settings to protect minors, and that in Canada, TikTok strives to partner with not-for-profit organizations in its efforts to educate young people about topics such as algorithmic bias.

Contradicting TikTok, Mr. Malone said that TikTok—like many other social media apps—is responsible for privacy violations, that it engages in improper data harvesting and narrative control practices, and that it grants access to data despite assurances otherwise.

According to Mr. Malone, TikTok—like other social media apps—is a "vector for online harm" inflicted on young people. He supported this statement by citing TikTok's business

26 Ibid., p. 3.

27 Ibid.

28 See also: ETHI, *Evidence*, de Eyre; ETHI, *Evidence*, David Lieber (Head, Privacy Public Policy for the Americas, TikTok).

29 TikTok, *Written response submitted to ETHI*, p. 4 [HYPERLINK NOT AVAILABLE].

model as being focused on privacy-invasive, targeted advertising that exacerbates the mental health crisis affecting young people, as well as the app's safety features for children that are easy to bypass. Mr. Malone stated that through various access to information requests, he has seen several internal briefings where Canadian government officials had identified these problems.

Meta's Practices: the platforms' position

The Cambridge Analytica Case

In 2019 the Office of the Privacy Commissioner of Canada (OPC) released an investigation report jointly with the Information and Privacy Commissioner for British Columbia concerning Facebook in the Cambridge Analytica case. Following this joint investigation, the OPC made recommendations, as it does not have the power to issue orders. The OPC brought the matter before the Federal Court, requesting that it issue the order it recommended. This is a "de novo" proceeding.[30] The Commissioner explained that the Federal Court dismissed the application by the OPC, which appealed on the two fundamental issues raised before the Court: consent and security measures.

Regarding Cambridge Analytica, Ms. Curran reiterated Facebook's position, essentially that there was no evidence Canadians' information was shared with Cambridge Analytica, adding that Meta does not sell its user data. She said the Federal Court had found that there was insufficient evidence Canadians' data was shared and that Facebook's data-sharing practices were adequately disclosed.

On 9 September 2024, the Federal Court of Appeal issued a unanimous decision, *Privacy Commissioner of Canada v. Facebook Inc.* 2024 FCA 140, reversing the Federal Court's decision and finding that Facebook's practices between 2013 and 2015 breached the *Personal Information Protection and Electronic Documents Act* (PIPEDA)'s requirement that it obtain meaningful consent from users prior to data disclosure and failed in its obligation to safeguard user data. The Federal Court of Appeal required the parties to report within 90 days of the date of the decision as to whether there was agreement on the terms of a consent remedial order. The Privacy Commissioner of Canada said he expects Facebook to now bring forward proposals on how it will ensure that it complies with the Court's decision.[31] At the time of adoption of this report, Meta had not

30 Office of the Privacy Commissioner of Canada (OPC), *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia*, Report of findings, 25 April 2019; *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2023 FC 533 (CanLII).

31 OPC, *Statement by the Privacy Commissioner welcoming the Federal Court of Appeal's decision on Facebook*, 9 September 2024.

indicated whether it intended to file an application for leave to the Supreme Court of Canada to appeal the decision. It has 60 days to file a leave to appeal after the appellate court's judgment.[32]

The Committee looked into Cambridge Analytica at the time that the OPC and the Information and Privacy Commissioner for British Columbia were investigating Facebook. First, the Committee released an interim report, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*. This was followed by a final report, *Democracy under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*. Both reports contained recommendations for legislative amendments concerning social media platforms, foreign financing and foreign influence in Canadian elections, and the powers of the Privacy Commissioner.[33]

Privacy

Ms. Curran argued that Meta has totally overhauled its privacy practices over the past few years and that privacy considerations are now embedded at the front end of the design of all of its products and services.

Regarding the new tools and features developed by Meta in recent years for teens and families, Ms. Curran gave the example of teens' accounts set to "private" when they join Instagram or Facebook. She told the Committee that Meta prevents adults whom teens do not follow from sending them messages and limits the amount of potentially sensitive content they can see in "Explore," "Search" or "Reels". Ms. Curran added that Meta prohibits content that promotes suicide, self-harm or eating disorders.

Countering External Threats

Mr. Gleicher said that Meta is working to identify and counter foreign adversarial threats, including hacking campaigns and cyber-espionage operations, as well as influence operations, what it calls coordinated inauthentic behaviour (CIB), which it defines as any "coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation."

32 *Supreme Court Act*, sections 40 and 58(1).

33 See also: ETHI, *International Grand Committee on Big Data, Privacy and Democracy*, June 2019. The International Grand Committee was made up of members from the Committee as well as parliamentarians from 10 other countries, and held meetings during which it heard from numerous witnesses, including experts, academics, regulators and digital platforms.

Mr. Gleicher told the Committee that CIB occurs when users coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. He said that Meta's community standards prohibit inauthentic behaviour, including by users who seek to misrepresent themselves, use fake accounts or artificially boost the popularity of content. According to Mr. Gleicher, this policy is intended to protect the security of Meta user accounts and services and to create a space where individuals can trust the people and communities they interact with.

Mr. Gleicher said that threat actors are seeking to interfere with and manipulate public debate, exploit societal divisions, promote fraud, influence elections and target authentic social engagement across the Internet. Mr. Gleicher said that the security teams at Meta have developed policies, automated detection tools and enforcement frameworks to tackle deceptive foreign and domestic actors. He said that these investments have enabled Meta to stop millions of attempts to create fake accounts every day and to detect and remove millions more. He gave the example of almost two billion fake accounts disabled by Meta in 2023, with more than 99% of them identified proactively before receiving any report.

Mr. Gleicher said that Meta investigates and hunts for cyber-espionage campaigns and that it regularly reports on that work in its quarterly reports, which describe the enforcements taken. Meta also shares information about any identified operations with others in the industry so they can take action as required.

According to Mr. Gleicher, Meta has seen that these cyberespionage campaigns are broad efforts that target the Internet broadly and often involve off-platform activity as well. Mr. Gleicher added that details on countries or regions that were significantly targeted are included in quarterly threat reports and that when Meta does have proof, it also publishes information about who or what organization was behind the operation.

Dr. Hundley told the Committee that the company uses a behaviour-based approach to identify covert influence operations, rather than one based on the content shared by bad actors. She said that Meta removes networks like these regardless of who is behind them, what they post, or whether they are foreign or domestic.

As an example, Dr. Hundley said that Meta has taken down more than 200 covert influence operations from 68 countries in at least 42 languages. She said that Meta regularly reports these kinds of information through its adversarial threat reports and that sharing this information has enabled its teams, investigative journalists, government officials, and industry peers to better understand and expose Internet-wide security risks, including ahead of critical elections.

Dr. Hundley said that as of Meta's latest report, China is now the third most common geographic source of foreign CIB that Meta has disrupted, after Russia and Iran. She noted that in 2023, Meta took down five CIB networks from China, more than any other country. According to Dr. Hundley, these CIB operations typically posted content related to China's interest in different regions worldwide, such as by praising China, defending its human rights records in Tibet and Xinjiang, or criticizing critics of the Chinese government, including journalists and researchers.

As indicated above, Dr. Hundley argued that countering foreign influence operations is a whole-of-society effort. She said that no single social media platform can solve the problem of foreign interference on its own, which is why Meta is working with its industry peers, independent researchers, investigative journalists, government and law enforcement.

X's Practices: the platforms' position

Mr. Fernández told the Committee that X users can choose to create a pseudonymous account in order to protect their identity or control who can see their posts. He said that X is guided by the principle that data should only be used for the purpose for which it was collected.

Mr. Fernández said that the account settings on X allow users to make a variety of choices about their data privacy, including limiting the data that X collects, determining whether they want to see interest-based advertising, and controlling how X personalizes their experience. He also said that X allows users to access information about advertisers that have included them in tailored audiences to show them ads, demographic and interest data about their accounts from ad partners, and information X has inferred about them.

Mr. Fernández argued that privacy by design is a priority with every product built by X. He said that X executes comprehensive privacy reviews for all new features and tools it rolls out. It also performs additional data protection impact assessments for products that may pose additional risks to its users.

Mr. Fernández added that X has taken steps to mitigate the unauthorized scraping and harvesting of data on its platform. He cited the use of dedicated teams that monitor, identify and mitigate scraping activity across a range of vectors and platforms; the introduction of rate limits to limit a malicious actor's ability to scrape data; the expansion of user verification offerings to assess whether a given account applicant is a

real person, not a bot; and updates to X's terms of service, which explicitly state that scraping is an express misuse of the X service.

Mr. Fernández told the Committee that even just using X means that the company receives personal information about its users, such as the type of device used and the IP address. According to Mr. Fernández, users can choose what additional information to share with X, including their email address, phone number, address book contacts and public profile. He argued that X uses this information to keep accounts secure and to show users more relevant posts to follow, such as events and ads.

Mr. Fernández acknowledged that X's business is largely based on advertising, but stressed that there are some fundamental differences between X and many other companies with a similar business model. According to Mr. Fernández, in general, rather than focusing on who the users are, X's data is more about what they are interested in, such as what they repost, what they like and whom they follow, all of which is public information.

Collection of Biometric Data

Josh Harris, Senior Privacy and Data Protection Counsel at X, said that the biometric data referred to in X's updated privacy policy is information that might appear on someone's ID card. As this information is more sensitive than others, more restrictions apply to its storage. He clarified that this data is not being used by X to train AI systems or any other technology. According to Mr. Harris, X uses biometric data to prove identity, for example, when parental consent is required for a person to create an account.

In a written response to questions put by the Committee to X representatives during their appearance, Mr. Fernández confirmed that X may collect biometric data from government-issued photo IDs for security and general verification purposes. He said that X collects this data for its investigations and policy enforcement, including when the consent of a parent or legal guardian is required, or when a case of identity theft is reported. There is also a voluntary identity verification process for certain features on the X platform. X's written response states that it currently has no plans to extend the collection of biometric data beyond these categories.[34]

34 X Corporation, *Written response submitted to ETHI*, 22 December 2023, p. 2 [HYPERLINK NOT AVAILABLE].

Google's Practices: the platforms' position

Privacy

According to Ms. Patell, Google builds products and services that are secure by default and private by design. She said that Google has made it publicly clear that a majority of its revenue is built upon advertising. She also said that Google's commitment to its users is to give them visibility into "how their information is informing their experience on [its] services, to give them tools for transparency and to ultimately put them in control in how their information is being used."

Ms. Patell said that the information collected by Google ultimately helps make its products function properly and effectively, makes them more secure, gives the ability to detect and mitigate fraud, and makes them more helpful. She said that Google provides settings for users to choose how their information is being collected and used. Google has something called the "privacy checkup centre," where individuals can see how this information is being used on "My Ad Center." Users also have the opportunity to either delete that information or turn off things like personalized advertising.

Ms. Patell told the Committee that Google provides information to users about the deletion of information or the deactivation of certain parts and has implemented an auto-delete function for new accounts, ensuring that information is automatically deleted after 18 months.

As for the content policies on YouTube, Ms. Patell said that the community guidelines apply to all content on the platform: comments, external links, the video itself, etc. She said that Google has over 20,000 trained reviewers in trust and safety who assess whether each piece of content on the platform meets the standards of Google's community guidelines.

Ms. Patell said that Google protects users' privacy with "industry-leading security infrastructure, responsible data practices and easy-to-use privacy tools" that put its users in control. She said that tools such as privacy checkup and security checkup send users personalized privacy and security reminders and recommendations, including flagging actions that they should take to immediately secure their Google account. In her view, these two verification functions allow users to customize, step by step, the security and confidentiality controls based on their personal preferences.

Ms. Patell also referred to the advanced protection program, which is available to anyone but is designed for individuals and organizations—such as elected officials,

political campaigns, human rights activists, and journalists—who are at a higher risk of targeted online attacks.

Ms. Patell explained that the processing of user data at Google includes protecting data from third parties and that it is Google policy to never sell its users' personal information to anyone.

As for the protection of minors, Ms. Patell said that YouTube is designed for users 13 years of age and older and that a birthdate must be provided in order to open an account. She said if a user indicates that they are under the age requirement, that attempt is blocked and there are no take-backs. The user is then funnelled through to YouTube's parental supervision process.

Countering External Threats

According to Ms. Patell, Google invests significantly in global teams and operations to prevent abuse on its platforms, such as the threat analysis group, headed by Shane Huntley, its senior director. He explained that Google's global team of analysts and security experts works closely with product teams to analyze and counter threats to Google and its users, including threats from government-backed attackers, serious cybercriminals and information operations.

Mr. Huntley said that on any given day, the threat analysis group tracks more than 270 targeted or government-backed attacker groups from more than 50 countries. He also said that Google publishes a quarterly bulletin about actions taken against accounts that appear to be linked to coordinated influence campaigns. He cited the third quarter of 2023, whose quarterly bulletin reported influence campaigns blocked by Google originating from Russia, Iran, China and Mexico.

Mr. Huntley told the Committee that the group he leads is particularly focused on disrupting coordinated influence operations on YouTube. He said that since January 2023, Google terminated more than 2,400 YouTube channels linked to Russia and more than 60,000 channels linked to China. According to Mr. Huntley, these actions are in addition to YouTube's ongoing enforcement of community guidelines, which resulted in the removal of more than eight million videos globally in the third quarter of 2023.

Mr. Huntley said that as Google discovers and disrupts operations, it takes steps to protect its users, disclose information publicly and share its findings with industry and government partners "to support the entire ecosystem." Google also issues warnings to its users when they appear to have been targeted by a government-backed attack.

CHAPTER 2: SOCIAL MEDIA PLATFORMS AND FOREIGN ACTORS

Use of Social Media Platforms by Foreign Entities

Cherie Henderson, Assistant Director, Requirements, Canadian Security Intelligence Service (CSIS), told the Committee that foreign state actors leverage all means to carry out their foreign interference activities, including social media platforms. For example, Russia and China use social media and their suggestive algorithms to amplify echo chambers and manipulate content presented to the public in order to spread disinformation.

Ms. Henderson explained that threat actors are interested in social media platforms for the data they generate and collect, including personal data such as photo albums, messages and contact lists. When collated on a massive scale, this data can provide trends and insights into populations, public opinion and individual networks.[35] This makes it important for Canadians to be aware of the privacy considerations at play when they choose to share their personal information online, especially with foreign-owned companies based outside of Canada or allied countries.

Ms. Henderson added that authoritarian states like China leverage big data to carry out foreign interference activities. They do not respect the ethical or legal obligations in place in other countries such as Canada. She believes that new technologies simply assist China in its nefarious activities. Ms. Henderson noted that the Chinese 2017 National Intelligence Law that compels individuals, organizations and institutions, including social media platforms operating in China, to provide mass information to the government assists Chinese security and intelligence services in carrying out their activities.

Mr. Khoury confirmed that in its unclassified national cyber-threat assessment 2023–24 report, the CCCS assessed that foreign states are using social media to target Canadians.[36] Mr. Khoury added that certain states are very likely using foreign-based social media and messaging applications popular with the diaspora groups in Canada and around the world to monitor communications. He said that certain states can take advantage of permissive terms of use and their own legislative powers to compel data sharing.

35 ETHI, *Evidence*, Cherie Henderson (Assistant Director, Requirements, Canadian Security Intelligence Service).

36 Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023–2024*.

Ms. Henderson stressed that hostile states are able to harvest personal information posted publicly on social media by individuals, pointing out that China is not alone in engaging in such activities. She said that it is important to not lose sight of all the hostile activity directed against Canadians by focusing on just one actor. She said that hostile states such as Russia, Iran and North Korea are able to crunch big data and engage in surveillance if they wish.

Ms. Henderson stated that in 2023, the Minister of Public Safety issued a ministerial directive indicating that if CSIS became aware of negative activities directed against politicians by hostile foreign states, then it must look at the information, determine its threat value and then reach out and advise the various political actors involved.

Ms. Henderson explained that foreign interference occurs all the time, not only during an election. CSIS is constantly monitoring what is happening to see if there is any type of foreign interference by a hostile state actor. It does not, however, monitor social media. The threat of foreign interference on social media must be real before CSIS takes action. It takes a very long time for CSIS to figure out where an attack came from, said Ms. Henderson. She also stressed the importance of guarding freedom of expression; when a threat comes from a foreign state, it is important to determine whether it is causing an impact on Canada's sovereignty and national security.

Peter Madou, Director General, Intelligence Assessments, at CSIS, said that the organization provides general advice to government on foreign interference. He said that CSIS investigates threat actors, not social media platforms. He stressed that detecting counter-narratives on social media platforms may be a common occurrence, but to link them specifically to a hostile threat actor is a bit more complex. This makes it difficult to know how often such a threat occurs.

Ms. Henderson also said that given just how much personal information is shared on social media, hostile foreign actors can get a very good picture of who you are and how they might be able to influence you. By monitoring social media, foreign actors can also pick up trends in a certain region, such as who people are voting for or what they are worried about. However, she said that by not sharing personal information, or by being careful about what is shared, it is possible to protect your social media presence.

Mr. Larkin said that the exploitation of the personal data of Canadian citizens by foreign actors and the commission of crimes in the digital space are of the highest priority for the RCMP. He noted that foreign interference affects many aspects of our lives, from the foundations of Canada's democracy and economic prosperity to the fundamental rights and values that define us as a society.

Mr. Larkin told the Committee that foreign actors seek to advance their objectives in a myriad of ways, including through harassment and intimidation of individuals and communities across Canada. These foreign actors are backed by a state. Foreign governments are leveraging data harvested through social media platforms to profile individuals and conduct misinformation and disinformation campaigns within Canada or identify and repress political dissidents who seek refuge in Canada.

Mr. Larkin said that the RCMP is mandated to investigate serious and organized crime and national security matters, which include instances of online foreign interference. Its National Cybercrime Coordination Centre works with all law enforcement and other partners, including the Canadian anti-fraud centre, to help reduce the threat from cybercrime within Canada.[37]

Mr. Larkin noted that in 2022, 35% of the (more than) 30,000 reports of cyber-enabled fraud and scams were linked to social media platforms. The RCMP is also working closely with police services across the country, as they are often the first law enforcement entities to learn about state-backed cybercriminal activities targeted at Canadians.

According to Mr. Larkin, it is critical for Canadians to understand that everything they share is collected and stored on servers, which are often located outside Canada, where privacy rights may not have the same meaning as they do here. He stressed the following:

> In some foreign jurisdictions, national security laws oblige social media companies to share this personal data collected from international users with local governments. This data is then used to harass, coerce and/or threaten dissenting voices, political leadership and our diverse communities abroad, and/or to facilitate cybercriminal activities.

Ms. Gauvin added that China and other foreign actors target dissidents and conduct foreign interference activities using a variety of means, including social media.

With regard to the data of Canadian citizens being hosted on foreign servers, Mr. Larkin said that the level of security of this information depends on several factors, such as encryption levels. However, he did say that no system can guarantee total data security.[38]

---

37 The Canadian Anti-Fraud Centre is jointly managed by the Royal Canadian Mounted Police, the Competition Bureau of Canada and the Ontario Provincial Police.

38 ETHI, *Evidence*, Bryan Larkin (Deputy Commissioner, Specialized Policing Services, Royal Canadian Mounted Police).

Mr. Larkin indicated that another challenge is the amplification of social media around involvement in criminal investigations. In the majority of the RCMP's investigations, anywhere from low-threshold crime to violent crime or exploitation, there is some form of digital entity tied to it. This is far from an investigation in a neighbourhood or schoolyard. The RCMP now sees cases where foreign actors are using and amplifying content on social media to target Canadian citizens and/or citizens who are living from abroad in our country, posing a significant challenge for the RCMP.

Mr. Larkin said that the RCMP does use social media as part of investigations in order to collect open-source information. They also use software to refine the searches required as a part of its routine work or criminal investigations.

Ms. Gauvin acknowledged that there has been an increase in foreign interference in recent years and that social media is being used as a vehicle for foreign entities to propel their activities. She said that this interference is much more difficult to detect.

However, Ms. Gauvin stressed that the RCMP does not investigate social media and is not looking to see if there is misinformation, disinformation or influence on the platforms. What the RCMP's national security program does is investigate criminal activities. If the criminal activities pertain to foreign interference, then an investigation will take place.

On the RCMP's ability to act in cases where content or an app was created in another jurisdiction, Ms. Gauvin said that "if a Canadian is threatened or the Canadian public safety or national security of Canada is threatened, that gives [the RCMP] the authority to act."

Data Scraping by Foreign Actors

Regarding the possibility of people's data being scraped and collected by foreign governments for nefarious purposes, Mr. Dufresne said that he and his provincial counterparts recently issued a statement on data scraping.[39] They asked social media organizations to take steps to protect data and to inform their users, as well as describe what individuals can do to protect their data.

Mr. Dufresne said that the statement addressed some of the risks related to data scraping, including "targeted cyber-attacks, identity fraud, monitoring, profiling and surveilling of individuals, unauthorized political or intelligence-gathering purposes, or

39 OPC, *Joint statement on data scraping and the protection of privacy*, 24 August 2023.

unwanted direct marketing or spam." The commissioners also outlined risk mitigation techniques that social media companies can and should implement to protect information from malicious actors who might scrape it.

On this point, Dr. Gruzd argued that there is reason to worry about the potential for TikTok and other platforms to be exploited by malicious actors for propaganda and radicalization. Dr. Gruzd's concerns are not limited to any one platform; rather, they represent broader challenges to the integrity and security of our information environment. He said that state actors will use all tools available and all social media platforms that are popular in Canada.[40] He said that focusing on just one platform makes it sound as though other platforms are safe when, in fact, they engage in similar data-harvesting practices and similar data misuse, or may be used by state actors.

Dr. Gruzd acknowledged that social media tools have been weaponized by various state actors and other interest groups attempting to shape public opinion. He added that these efforts are sometimes carried out by large, automated bot networks. For example, research conducted with data provided by Twitter found that automated bots posted innocent content on sites like X, later on switching to different narratives. State actors tap into division and polarization, overtly or covertly.

Dr. Gruzd added that there are different types of foreign interference. There are platforms where a state actor has direct access, such as VKontakte, which ran from Russia and had to be banned in Ukraine since it was determined that it was actually run by the State. Sometimes, data is accessed through developers' apps, which is another form of interference.

Dr. Gruzd said that state actors often target sympathetic groups, which will, for example, repeat the content they provide such as pro-Kremlin content. They look at political partisan views that may be aligned with their objectives. The goal is to have the content impact someone in power, such as a TikTok influencer or politician running for office, who will usefully share the desired narratives.

It is concerning that more Canadians turn to social media for information about conflicts like the war in Ukraine or the war in Palestine, when reactions on these platforms are driven by the content produced by the influencer providing the news, as Dr. Gruzd pointed out. He believes that credible news sources simply cannot compete with influencer content. While "freedom of speech" is important, he pointed out that it is just

40 ETHI, *Evidence*, Gruzd.

as important to make sure that Canadians participating in these platforms have access to credible information.

TikTok: Data Overcollection and Potential Sharing with Foreign Actors

Investigations into TikTok and Fines by Authorities in Other Countries

In February 2019, the U.S. Federal Trade Commission (FTC) announced that the app Musical.ly (now TikTok) had agreed to pay US$5.7 million to settle a complaint that the company had illegally collected personal information from children in violation of the *Children's Online Privacy Protection Act*, which requires parental consent for the collection of personal information on children under the age of 13. TikTok argued that the settlement does not mean there was a finding of a violation or a breach and that since 2019, TikTok has implemented a number of default settings, safeguards and tools to protect minors, including Canadian teens.[41]

In September 2023, the Irish Data Protection Commission (the DPC or the Irish Commission) fined TikTok €345 million for violations of various articles of the European Union (EU) General Data Protection Regulation (GDPR) in relation to its processing of personal data relating to children.[42] Mr. Lieber said that TikTok disagreed with the DPC decision and fine and has launched an appeal. He explained that the fine was in relation to settings for younger users whose accounts were created prior to 2020. He added that at the time the investigation commenced, TikTok had already implemented protocols to make certain teenagers' accounts private by default and introduced other settings for minors.

In April 2023, the UK Information Commissioner's Office fined TikTok £12.7 million for violating a number of provisions of the *Data Protection Act 2018*, including for providing services to children under the age of 13, processing their personal data without consent or authorization from their parents or guardians, and for failing to provide proper information to TikTok users about how their data is collected, used and shared in a way that is easy to understand. TikTok disagreed with the UK Information Commissioner's

41 TikTok, *Written response submitted to ETHI*, p. 9 [HYPERLINK NOT AVAILABLE].

42 Irish Data Protection Commission, *Irish Data Protection Commission announces €345 million fine of TikTok*, 15 September 2023.

Office decision. As with the fine imposed by the Irish Commission, the decision covers a period prior to 2020, and TikTok is appealing the decision.[43]

Joint Investigation of TikTok by Canadian Authorities

Mr. Dufresne told the Committee that he had opened a commissioner-initiated complaint against TikTok in February 2023. The joint investigation is being conducted with his provincial counterparts in Quebec, Alberta and British Columbia. During his appearance in October 2023, Mr. Dufresne said they are looking forward to completing their investigation by the end of March 2024. No investigation report has been published yet. The Commissioner said that the focus of the joint investigation is on TikTok's data practices, including consent for appropriate purposes, with a particular focus on children and youth, because they are the majority of the users.

Mr. Dufresne said that the commissioners are also looking at whether a reasonable person would consider the purposes for which TikTok handles personal information, in particular children's information, to be appropriate in the circumstances, namely that the use of such data is for "appropriate purposes", the term used in PIPEDA. The investigation will also determine whether TikTok is meeting its transparency obligations, particularly when collecting personal information from its users.[44]

The Commissioner could not go into the details of the investigation, which is ongoing. What Mr. Dufresne did say was that the investigation was initiated in the wake of class-action lawsuits in the U.S. and Canada, as well as numerous media reports related to TikTok's collection, use and disclosure of personal information. He also addressed the privacy principles that underpin the OPC's approach to the digital world from the perspective of the privacy rights of children.

Michael Maguire, Director, PIPEDA, Compliance Directorate, at the OPC, confirmed that the investigation involves ByteDance as the owner of TikTok. Mr. Dufresne also said that under PIPEDA, an organization is responsible for personal information in its "custody, including information that has been transferred to a third party for processing." In so doing, the organization "shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party." Bill C-27,

43 TikTok, *Written response submitted to ETHI*, p. 9 [HYPERLINK NOT AVAILABLE].

44 ETHI, *Evidence*, Philippe Dufresne (Privacy Commissioner, Office of the Privacy Commissioner of Canada).

which is discussed in Chapter 3, contains a similar obligation in section 11 of the proposed Consumer Privacy Protection Act (CPPA).[45]

Mr. Dufresne said that in the case of data sharing, it is important to check whether it is appropriate, whether it respects legal limits and whether it gives rise to security concerns. He said that the OPC has a number of tools to assess an organization's practices, such as site visits and requests for documentation. The OPC also has a lab with technical tools to investigate digital material and obtain the information they need. Mr. Maguire told the Committee that the OPC also has the ability to interview under oath as well as to visit a site to require the production of documents.

In its written response, TikTok says that the privacy and safety of its users, particularly its younger users, are always a top priority, and it is cooperating with the Canadian data protection authorities in the investigation.[46]

A National Security Review of TikTok

On 6 September 2023, the Government of Canada issued an order for the national security review of TikTok.[47] The office of the Minister of Innovation, Science and Industry stated that the review was not disclosed—and the cabinet order is not accessible—because the information is protected and confidential under the *Investment Canada Act*.[48] The Minister's office also indicated that TikTok would be subject to "enhanced scrutiny" under the Act through a new policy on foreign investments in the interactive digital media sector, which was released by the government at the beginning of March 2024.[49] That policy statement states that "hostile state-sponsored or influenced actors may seek to leverage foreign investments in the interactive digital media sector to propagate disinformation or manipulate information in a manner that is injurious to Canada's national security."[50]

---

45 Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Bill C-27).

46 TikTok, *Written response submitted to ETHI*, p. 8 [HYPERLINK NOT AVAILABLE].

47 Anja Karadeglija, "Federal government reveals it ordered national security review of TikTok", 14 March 2024.

48 See Part IV.1 of the *Investment Canada Act*, "Investments Injurious to National Security" (s. 25.1 to 25.6).

49 Government of Canada, *Policy Statement on Foreign Investment Review in the Interactive Digital Media Sector*, 1 March 2024.

50 Ibid.

In a letter Innovation, Science and Economic Development Canada sent to the Committee on 12 April 2024, it is indicated that a national security review can last over 200 days. It also states that for reviews resulting in a final Governor-in-Council order, a notice of the decision is published in a monthly listing that is made available to the public and the media. At the time of the adoption of this report, no such public notice had yet been published with respect to the national security review of TikTok.

TikTok Bans in Other Countries

There is a total ban on using TikTok in certain countries, such as India, Indonesia and Pakistan.[51] In other countries, such as Canada, the United States, European Union member countries, the United Kingdom—in addition to its parliament—Australia and the Parliament of New Zealand, the ban is limited to government devices.[52]

On 23 February 2023, the European Commission—the executive branch of the European Union—suspended the use of TikTok on employees' devices "to protect the Commission against cybersecurity threats and actions which may be exploited for cyber-attacks against the corporate environment of the Commission."[53] The Commission added that the security developments of other social media platforms will also be kept under constant review.[54]

On 27 February 2023, the Canadian government announced that, effective 28 February, the use of TikTok would be banned on government-issued mobile devices.[55] This decision was based on a review of TikTok by the Chief Information Officer of Canada, who determined that it presented an unacceptable level of risk to privacy and security.[56]

---

51 French Senate, *Rapport fait au nom de la commission d'enquête (1) sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence*, 4 July 2023, p. 9 [IN FRENCH].

52 United Kingdom, Cabinet Office, *TikTok banned on UK government devices as part of wider app review*, News release, 16 March 2023; Australia, Attorney-General's portfolio, *TikTok ban on Government Services*, News release, 4 April 2023; Sapna Maheshwari and Amanda Holpuch, *Why Countries Are Trying to Ban TikTok*, *The New York Times*, 16 August 2023.

53 European Commission, *Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices*, News release, 23 February 2023.

54 Ibid.

55 Government of Canada, *Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices*, 27 February 2023.

56 Ibid.

On 27 February 2023, the White House gave federal agencies 30 days to remove the app from U.S. government devices and systems.[57] TikTok had already been banned three years earlier on U.S. government devices used by the military.[58]

Mr. Lieber confirmed that negotiations are ongoing between TikTok and the Committee on Foreign Investment in the United States regarding an agreement to mitigate national security concerns posed by the platform to the U.S. He said that in the meantime, TikTok has put in place Project Texas, which endeavours to address the concerns that the U.S. government has raised, mainly the concerns about Chinese government access to user data and how the platform may be manipulated or used.[59]

In April 2024, the *Protecting Americans from Foreign Adversary Controlled Applications Act* was passed in the U.S. by the adoption of an appropriation bill to provide supplementary appropriations to several U.S. federal agencies for assistance to Ukraine, Israel and U.S. allies in the Indo-Pacific region. The Act requires that within 270 days of its adoption, TikTok must be sold to a non-Chinese owner. Failure to do so would lead to the banning of the application in the United States. Deadline for such divestment is 19 January 2025.

TikTok Ban on Canadian Government Devices

Catherine Luelo, who was a Deputy Minister and Chief Information Officer of Canada at the time of her appearance, said that she never felt any political pressure to ban the app.[60] She said that the government had recently banned WeChat and Kaspersky Lab, in addition to TikTok.

Ms. Luelo said that her role makes her accountable for ensuring that the government has clear rules and guidelines around the usage of government devices. That is the purview through which she made the decision on TikTok. She explained that when making decisions around what acceptable use is in government devices, consideration needs to be given to a whole series of issues, such as privacy, what is acceptable use in business environments, and cost.

57 David Shepardson, *White House sets deadline for purging TikTok from federal devices*, Reuters, 28 February 2023.

58 Stephen Castle, "U.K. Bans TikTok on Government Devices," *The New York Times*, 16 March 2023.

59 TikTok, U.S. Data Security, *About Project Texas*.

60 ETHI, *Evidence*, Catherine Luelo (former Deputy Minister and Chief Information Officer of Canada)

Ms. Luelo told the Committee that it is important to continue tightening the environment in terms of the use of government devices, which she said is fairly open at the moment. About 90% of government devices allow users to download whatever they like and allow business and personal use on the same device. She advised the government to ensure that devices are used only for government business.

Ms. Luelo did acknowledge that in some cases, there may be an acceptable reason to use a social media platform for business purposes, such as to reach a certain type of individual who uses social media to get information. She gave the example of using social media platforms to reach out to demographic groups about COVID vaccines during the pandemic. For Ms. Luelo, the risk is acceptable when "the value of doing the thing outweighs the risk of any potential downside."

Mr. Khoury explained that when providing advice and guidance on what is downloaded on government devices, the CCCS looks at a number of things, such as security controls and who is behind the app. He said that that foreign threat landscape is informed by a number of sources, some of them public and some classified. He listed off the CCCS's concerns: Who has access to the data? Where does the data reside? How easy is it for the host nation to get access to the data? In the case of TikTok, if the data is hosted in China, that would be a concern, considering China's laws allowing access to user data.

Regarding the decision to ban TikTok on government devices, Mr. Khoury said that although the CCCS was part of the round table with the Treasury Board Secretariat, the decision to ban the app belongs to the Chief Information Officer.[61]

Along those same lines, Mr. Dufresne said that the Government of Canada made decisions based on its review, which was based on advice from the Chief Information Officer and various subject matter experts. He confirmed that he was not involved in the government assessments that resulted in the ban. He said that governments have a responsibility for national security and the security of public servants' information.

Dr. Gruzd pointed out that banning a single app may not be effective. Such a ban could also undermine trust in government, legitimize censorship and create an environment for misinformation to thrive. In his view, unless there is clear evidence of foreign interference, banning a platform undermines our democratic processes by creating a perception of politicization of this topic.

61 ETHI, *Evidence*, Sami Khoury (Head, Canadian Centre for Cyber Security, Communications Security Establishment).

Similarly, Mr. Malone found that the statement about concerns relating to privacy and security that accompanied the ban on using TikTok on government devices raised several unanswered questions. He pointed out that TikTok is not the only app that retains user data in foreign jurisdictions and potentially shares it with foreign regimes.

Mr. Malone stated that he received confirmation from the Treasury Board Secretariat that none of the following apps are banned from download and use on government-issued devices: Russian-affiliated VKontakte, Yandex and Mail.ru, as well as Facebook, Instagram, Tinder, Snapchat, Bumble, Grindr, Truth Social, Gab and Discord. Mr. Malone pointed out that Discord was implicated in the 2022–23 Pentagon Papers leaks and do not have child safety protection measures, according to Dr. Laidlaw.

Mr. Malone recommended that the government ban all social media apps on government-issued devices, unless there is a strong business justification otherwise, in the interest of better privacy and security. He also recommended that the government stop buying ads on all social media services.

Mr. Malone believes it is unethical to advertise with social media companies given the concerns raised about data harvesting and illicit foreign interference. He pointed out, for example, that in 2022, the Canadian government spent $141 million on advertising, including almost $2 million on TikTok.

With respect to the type of information being shared on government-issued devices, Mr. Malone said that even if using certain apps is harmless on an individual level, the data collected could potentially be useful in the aggregate. He explained that certain pieces of information like location data might reveal sensitive information such as the location of politicians or members of the Canadian Armed Forces.

Given the witnesses' concerns about how government devices are used, the Committee makes the following recommendation:

Recommendation 1

That the Government of Canada reevaluate its digital standards regarding the download and use of all social media apps on government-issued devices in order to ensure that they are used primarily for government business.

TikTok's Position on Being Banned

Regarding the TikTok ban on Canadian government devices, Mr. de Eyre said that TikTok has engaged with the Treasury Board Secretariat and the Office of the Chief Information

Officer to try to better understand what criteria were used to single out TikTok, while other platforms operate in a similar way. He recognized that while there is probably no need to have any social media, entertainment or gaming apps on a government employee's device, those rules should apply to all platforms.

Given that TikTok has been banned in countries such as India, Indonesia and Pakistan and its use on government devices is limited in countries and jurisdictions such as Australia, New Zealand and throughout the European Union, TikTok argued in its written response that these bans are misinformed and unmerited.[62]

TikTok officials believe that these bans do not point to any conclusive finding of a substantiated privacy violation or problem. In their opinion, singling out one company is not the correct approach for increasing the protection and safety of users. For example, in its written response, TikTok states that the platform's ban on Government of Canada devices risks having a negative impact on Canadians, since it shutters channels that government, public institutions and other authoritative voices were using to reach Canadians, and it stunts public discourse.[63]

Questions Surrounding the Corporate Control of TikTok

Mr. de Eyre insisted that TikTok's parent company, ByteDance, is not owned or controlled by the Chinese government; nearly 60% of ByteDance is owned by global institutional investors, 20% by its founders and 20% by employees. He said that three of the company's five board members are from the U.S. He acknowledged that ByteDance was founded in China, but he insisted that it is a global company with offices around the world.

Mr. de Eyre said that TikTok is not available in mainland China and that it is a private organization, not a state-owned enterprise. He also pointed out that ByteDance is a private company that is ultimately accountable to its board. He acknowledged that Douyin, a product similar to TikTok for the Chinese market, is also owned by ByteDance, adding that Douyin is a separate app. He added that TikTok is headquartered in Los Angeles and Singapore, that its general counsel is based in the U.S. and that its head of trust and safety is based in Dublin. Mr. de Eyre also said that TikTok has thousands of employees around the world, with 150 in its Canadian office in Toronto.

62 TikTok, *Written response submitted to ETHI*, p. 8 [HYPERLINK NOT AVAILABLE].

63 Ibid.

Mr. de Eyre confirmed that there is a Chinese operating entity specifically for the Chinese market, hastening to add that this entity has nothing to do with TikTok and has no oversight over TikTok, that its employees cannot access TikTok user data, and that it is not above TikTok in the org chart.

Regarding data sharing with the Chinese Communist Party, Mr. Lieber said the following:

> We've been quite clear that we would not disclose user data to the Chinese government if it made a request. It has not made such a request, and the Chinese government has not asserted the rights over any TikTok user data. The TikTok app itself is not available in mainland China. As we have discussed before, we have a Canadian operating entity in Canada. We have employees in Canada. We have users in Canada, and we're subject to Canadian law. We also have a biannual transparency report where we disclose the number of government requests that we receive from governments throughout the world. Therefore, if we did receive a request from the Chinese government, we would certainly disclose it in our transparency report.

Mr. Lieber said that he did not know whether the Chinese government has the technological capability to access user data directly, without requesting it. He argued that it would be irresponsible for any employee of a technology company to make categorical guarantees about what governments are or are not capable of in terms of their ability to conduct activities, including hacking.

Mr. Lieber also said that TikTok's privacy policy has a provision dealing with the sharing of information within its corporate group, noting that there are functions performed by other entities in the corporate family to which TikTok belongs, such as to troubleshoot an account. He pointed out that ByteDance has subsidiaries throughout the world and that it may be possible to argue that the Chinese law does not apply in regions of the world where there are no Chinese users.

However, Mr. Andrey told the Committee that The Dais put TikTok under particular scrutiny, given its corporate structure. He said that prior to 2019, TikTok's privacy policy was transparent in stating that it shares its users' information "with any member or affiliate of [its] group" in China. This specific location reference was subsequently removed, but the sharing provision remains. Mr. Andrey explained that this same provision also appeared in the privacy policy of WeChat —used by 6% of Canadians — and this is the case for many others.

Mr. Malone pointed out that TikTok has been caught engaging in all kinds of worrying conduct with respect to user data, such as accessing the physical locations of journalists using the app to track down their sources. He also told the Committee that TikTok directed data from its users in the U.S. through China despite assurances otherwise.

Mr. Malone cited internal government reporting from Canadian government actors like the Privy Council Office's intelligence assessment secretariat that identifies other problems around the type of data and the collection of data through TikTok.

Mr. Malone also told the Committee that he had an opportunity to review *Economic Security and Technology: TikTok Takeover*, a federal government document from the cyber-threat intelligence unit at National Defence that identifies concerns with respect to TikTok that include surveillance and intelligence operations, privacy violations, data harvesting, political interference, narrative control and Communist Party of China censorship exports. According to Mr. Malone, the brief also addresses concerns with respect to many other social media companies, such as Snapchat and LinkedIn.

CHAPTER 3: OVERSIGHT OF SOCIAL MEDIA PLATFORMS

Privacy

Currently, the federal privacy law that applies to the private sector is PIPEDA. It applies to federally regulated businesses, as well as to businesses operating in provinces that have not enacted substantially similar legislation.[64] PIPEDA was enacted in 2000.

In June 2022, the Government of Canada introduced Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.[65] The CPPA would replace Part 1 of PIPEDA.

In April 2023, Bill C-27 passed second reading in the House of Commons and was referred to the House of Commons Standing Committee on Industry and Technology.[66] Several witnesses referred to Bill C-27 as part of this study. These comments are reflected in this chapter. However, the recommendations in this report pertain to amendments to PIPEDA, as it is the legislation in force at the time of adoption of this

64 The three provinces with substantially similar legislation are Alberta, British Columbia and Quebec.

65 Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Bill C-27). See also: Sabrina Charland, Alexandra Savoie and Ryan van den Berg, *Legislative Summary of Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, Publication No. 44-1-C27-E, Library of Parliament, 12 July 2022.

66 House of Commons, *Journals*, 44th Parliament, 1st Session, 24 April 2023.

report. If adopted, Bill C-27 could remedy some of the shortcomings of the current legislative regime identified by witnesses.

Valid Consent

The issue of valid consent came up several times during the study. Mr. Dufresne said that Bill C-27 would strengthen valid consent by explicitly stating that this has to be provided in information that the person can understand.[67] However, Ms. Polsky said that the CPPA requires only that certain information be communicated in plain language, without a sufficient level of detail. The Privacy and Access Council of Canada (PACC), of which Ms. Polsky is president, believes that the CPPA confuses notification and consent.[68] She argues that the proposed consent rules in Bill C-27 and even those in the Quebec legislation, which was amended by Law 25, still leave organizations too much latitude.[69]

Regarding the privacy policies of organizations, Mr. Dufresne said that the OPC provides the following guidance: "Make it user-friendly. Make it not just a one-time thing. Make sure that you sometimes provide follow-ups. Make it as understandable as possible." He also suggested adapting the way consent is obtained when children are involved, such as by using a video rather than a written policy. He said that while it takes data to innovate, innovation can also be used to protect data and help ensure consent and explicability.

One example of innovation cited by Dr. Gruzd is the "Terms of Service; Didn't Read" initiative. It allows legal experts and technologists to evaluate the terms of service of various technological tool providers, including social media platforms. They assign ratings to these terms of service, which people can access online.[70] Dr. Gruzd said that all

---

67 Bill C-27, Consumer Privacy Protection Act (CPPA), s. 15. Section 15(3) of the CPPA provides that consent is valid only if the organization provided certain information to the individual. Section 15(4) states that this information must be provided in plain language. See also: Office of the Privacy Commissioner of Canada (OPC), *Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022*.

68 Section 6.1 of PIPEDA currently provides that the consent of the individual is only valid "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." See also: ETHI, *Brief*, Privacy and Access Council of Canada (PACC), para. 48. This brief presents PACC's comments and recommendations on Bill C-27.

69 Quebec National Assembly, Bill 64 (2021, chapter 25), *An Act to modernize legislative provisions as regards the protection of personal information* (Law 25). This law amended Quebec's *Act respecting the protection of personal information in the private sector*.

70 ETHI, *Evidence*, Gruzd. An extension installed on a web browser displays the rating given to a platform's or website's terms of use and spells out its shortcomings, for example whether the platform can access users' private messages or does not actually delete their data.

social media platforms, including TikTok, received the lowest grade by this initiative. However, Mr. Harris said he believes that X users reading its privacy agreement have the ability to understand what they are consenting to, including when it comes to the collection of biometric data.[71] The Committee notes that TikTok's terms of services are quite lengthy and written in legal terms. Its privacy policy is also lengthy.[72]

Other witnesses discussed privacy policies. For example, Mr. Caraway criticized the complexity of end-user licence agreements, which can only be understood by experts and can change on a daily basis, calling into question what consent actually means in this context. Mr. Khoury acknowledged that it would be helpful if the terms of use were explained in such a language that the app users understand what they are consenting to sharing and with whom.

Ms. Polsky believes the problem is that the social media platforms acknowledge that few people read their privacy policies. This tells her that they are collecting our personal information knowing that nobody reads the privacy policy, meaning that it is without informed consent. In her view, Canadian consumers should be able to access an index listing companies that comply with Canadian privacy legislation so they can make more informed choices about which companies they choose to share their information with.

The PACC and Sam Andrey have concerns about the exceptions to consent in the CPPA regarding "business activities" and "legitimate interest." These exceptions allow an organization to collect or use an individual's personal information without their knowledge or consent as part of business activities or when it has a "legitimate interest" to do so.[73]

Mr. Malone spoke about how difficult it is to talk about valid, informed consent given such a large power imbalance between individual users clicking "accept" on a lengthy privacy policy and a company with a market valuation that exceeds the size of a G7 country.

In fact, for Mr. Malone, informed consent, which is what Canadian privacy laws are based on, "doesn't serve the ends that we really need data protection and privacy law in this country to serve." He believes a fundamental shift in the paradigm is required so

71 ETHI, *Evidence*, Josh Harris (Senior Privacy and Data Protection Counsel, X Corporation).

72 TikTok, *Terms of Service*; TikTok, *Privacy Policy*.

73 PACC, s. 18. The activities covered by the "business activities" exception are listed in section 18(2) of the CPPA. What constitutes a "legitimate interest" is specified in section 18(3). To benefit from the exceptions in section 18, an organization must meet certain criteria or conditions precedent; See also: PACC, *Brief*, paras. 47–56, 59–63, 72–73.

that possessing, retaining, using or disclosing personal information becomes a liability, rather than a profitable way to run a business.

Legal Duties of Organizations

Mr. Dufresne said that there is often an economic incentive for digital platforms to use its users' information. States and regulatory bodies must therefore create incentives to protect personal information. He believes that there should be two kinds of incentives: a positive incentive, which recognizes good behaviour and gives reputation-related rewards; and a negative incentive, which uses legal constraint.

Mr. Dufresne believes that appropriate regulations would impose on platforms a proactive duty: to publish their privacy plan, to conduct audits, and to minimize data use. He would add a duty to properly explain how an organization uses the data it collects. Failure to fulfill these duties should result in audits, investigations, orders and fines.

Mr. Dufresne also said that PIPEDA is older than social media. In his view, as technology advances, stronger proactive obligations are needed. For example, organizations need to be forced to make basic assessments and report them to the OPC. There also need to be greater transparency requirements, particularly when it comes to the use of AI.

Data Minimization

Regarding data minimization, Dr. Gruzd said that parts of Bill C-27 could allow Canadians to request that their data be removed.[74] He noted that it is all too common for platforms to collect more data by default than necessary. In his view, the focus needs to shift from individual responsibility to the development of strategies that compel companies to implement privacy by design and by default.

Mr. Caraway said that considering the economic imperative to maximize data collection, legal criteria should limit data collection. He again pointed out that there is a propensity for overuse and exploitation of finite resources when there is unfettered access to them.

As a solution to data overcollection, Dr. Laidlaw proposed identifying no-go zones, certain forms of data collection that should be seen as wholly inappropriate and banned.

74 CPPA, s. 55 (right of removal). An individual may request the removal of their personal information, except where an exception applies. No exception may be used to refuse to remove the personal information of minors.

Dr. Laidlaw explained that users appear to agree to the harvesting of all kinds of personal information because they want to use an app.[75] She believes that people should not be able to agree to this kind of data collection since they do not really understand what they are agreeing to, such as their personal information being sold to data brokers. Once this data is in the hands of data brokers, it becomes impossible to know what happens to it.

Ms. Polsky also believes that we must fight the position taken by the Web giants, which insist that users want them to collect as much personal information as possible in order to create their profile. Since few people really understand what these companies are doing with their data, she disagrees with that position.

As for the ability of users to understand what happens to the data they provide to an online platform after it has been shared with a third party such as a data broker, Dr. Laidlaw said that California's *Online Privacy Protection Act* "basically [says] you need to be able to track that data and who it all goes to." She said that this legislation is more effective than Canadian legislation in terms of an individual's ability to know what happens to their personal information online.[76]

Order-Making Power and Administrative Monetary Penalties

Mr. Dufresne pointed out that under PIPEDA, the Privacy Commissioner can only make non-binding recommendations. This means that platforms are free to decide whether to act on the OPC's recommendations.[77] He said that if an organization is raking in millions or tens of millions of dollars using data and there are no monetary penalties when a contravention of the law occurs, it may be tempted to contravene the law again. In his view, the Privacy Commissioner not being able to issue orders or administrative monetary penalties is a major shortcoming of the current legislative regime.

Ms. Polsky is of the view that privacy regulators lack sufficient powers and funding.[78]

---

75 ETHI, *Evidence*, Brett Caraway (Associate Professor of Media Economics, University of Toronto).

76 California, *California's Online Privacy Protection Act*. The Act requires commercial websites and online services to post their privacy policy, which must indicate whether third parties may collect consumers' personally identifiable information to track them across different websites in order to profile their behaviour and interests. It must also indicate how the website or online service responds to Web browser "do not track" signals.

77 See also: ETHI, *Evidence*, Dufresne.

78 See also: PACC, *Brief*, paras. 56 and 70, 109–112.

The committee notes that Bill C-27 would give the Privacy Commissioner order-making powers. It would also give the Privacy Commissioner the power to recommend that a newly created Personal Information and Data Protection Tribunal impose administrative monetary penalties. The Privacy Commissioner, however, would not have the power to impose administrative monetary penalties under Bill C-27.[79]

Fines

Regarding fines, Mr. Caraway said that he supports the approach taken by Bill C-27, which provides for fines of up to 5% of the organization's gross global revenues in the preceding fiscal year.[80]

Ms. Polsky would go further. Pointing to the *Sarbanes-Oxley Act of 2022* in the U.S., which provides that the person at the head of the organization is responsible for everything in the financial statement, she recommended fines for CEOs instead of just the organizations.[81] She acknowledged that it may be useful to have both: fines on the organization and consequences for CEOs.

Codes of Practice and Private Right of Action

Mr. Dufresne said that Bill C-27 provides for the creation of codes of practice and certification programs.[82] In his view, this will encourage organizations to adhere to a series of rules, which will have a positive effect on the complaints process.[83] However,

79 Bill C-27, CPPA, ss. 93–95. Section 95 of the CPPA allows the Personal Information and Data Protection Tribunal (the Tribunal) to impose administrative monetary penalties for non-compliance with certain sections of the CPPA.

80 Bill C-27, CPPA, s. 128. Section 128 of the CPPA provides for a penalty if an organization contravenes specific sections of the Act (ss. 58, 60(1), 69, 75 and 127(1)) or obstructs the work of the commissioner. A breach of the CPPA can result in a fine imposed by the court followed by prosecution by the Attorney General of Canada.

81 The administrative monetary penalties and fines under the CPPA are imposed on organizations, not executives. Fines under PIPEDA are imposed on organizations.

82 Bill C-27, CPPA, s. 76. An entity may apply to the privacy commissioner for approval of a code of practice that provides for substantially the same or greater protection of personal information as some or all of the protection provided under the CPPA.

83 Bill C-27, CPPA, s. 87. A complaint may be inadmissible if the issue raised in the complaint concerns a certification program approved by the commissioner and the organization in question is certified (s. 87(1)(d) of the CPPA).

the PACC raised the possibility of this approach requiring an organization to comply with more than one code of practice, which would hamper compliance with these codes.[84]

Ms. Polsky was critical of the private right of action in the CPPA given that it becomes available only once the OPC complaints process and Tribunal appeals process have been exhausted.[85] PIPEDA does not contain a private right of action.

Cross-Border Data Transfers

Several witnesses were concerned about the lack of an explicit provision for cross-border transfers in PIPEDA and the CPPA, which would replace it.

Mr. Malone noted that neither PIPEDA nor Bill C-27 imposes any meaningful constraints on data transfers to jurisdictions like Russia and China. He said that cross-border data transfers are permitted under sections 11 and 19 of the CPPA.[86] He also said that an internal brief that he obtained through an access to information request confirms that the government chose to avoid putting cross-border transfer restrictions in Bill C-27 out of deference to commercial interests of the companies involved.[87]

The PACC also raised concerns about sections 11 and 19 of the CPPA. For example, according to the PACC, section 19, which allows the transfer of an individual's personal information to a service provider without their knowledge or consent, renders the right to withdraw consent under section 17 moot. It also makes it more difficult to exercise the right of withdrawal under section 55, since some of the individual's personal information may have been shared with a service provider or other party without their knowledge.[88]

As stated in Chapter 1, Mr. Masoodi said that there are currently inadequate protections over how Canadians' personal data is transferred and stored, particularly outside of

84 PACC, *Brief*, paras. 107–108.

85 PACC, *Brief*, paras. 121–122. Bill C-27, CPPA, s. 107.

86 Bill C-27, CPPA, s. 11(1). This section provides that an organization that transfers personal information to a service provider must ensure, by contract or otherwise, that the service provider provides a level of protection of the personal information equivalent to that which the organization is required to provide under the CPPA. The provider is not subject to the CPPA except with respect to sections 57 and 61 (security safeguards). Section 19 of the CPPA allows an organization to transfer an individual's personal information to a service provider without their knowledge or consent.

87 Matt Malone, *Reference document submitted to the ETHI Committee* [NO HYPERLINK AVAILABLE].

88 PACC, *Brief*, paras. 57–58 and 68–69, 92–93; Bill C-27, CPPA, ss. 11(2), 17, 19, 55(4), 57 and 61.

Canada. He therefore believes that robust privacy measures need to be in place, specifically with regard to cross-border data transfers.

Mr. Andrey similarly argued that as it currently stands, Bill C-27 allow for even easier data sharing by eroding what limited consent provisions do exist. He recommended that there be more precise requirements added to Bill C-27 to ensure that equivalent levels of protection are provided for data when it is transferred outside of Canada. He recommended requirements comparable to the GDPR.[89] He also raised the possibility of banning the transfer of minors' data to countries with insufficient equivalent protection.

Mr. Malone added that the GDPR requirements are stricter than those in Canada around data transfers and provide for a robust equivalency test.[90] However, he did point out that, unlike Europe, the U.S. has no uniform privacy legislation. They are exporting, through trade treaties and governance bodies worldwide, a view of data governance and privacy that affects what Canada can do. Mr. Malone cited as an example the Canada–United States–Mexico Agreement, which prohibits restrictions on cross-border dataflows. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership contains a similar prohibition.

Mr. Malone also raised the possibility of creating safe dataflow zones that would map onto existing security alliances such as NATO. Given the NATO allies' commitment to mutual defence, he believes that it would seem logical that we might feel comfortable sharing data and personal information with these allies in a free cross-border dataflow zone.

Applying Legislation to the Government and Political Parties

According to Mr. Malone, Canada needs privacy and data protection laws that show Canadians that the government is taking privacy and data protection seriously. This means having robust legislation that applies to government conduct. It also means that "political parties, which are often very eager to call out the privacy harms perpetuated by private social media companies," should be covered by Canadian privacy legislation.

---

89 Chapter 5 of the General Data Protection Regulation sets out requirements concerning the transfer of personal data to third countries or international organizations (arts. 44–50); See also: Stevens, Y., Masoodi, M.J. & Andrey. S, *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*, Cybersecure Policy Exchange, 2020. The report makes the same recommendation, adding that social media platforms should be required to obtain the explicit consent of Canadian users before transferring their personal data to States that do not offer a level of protection equivalent to Canada's.

90 The General Data Protection Regulation permits the transfer of data between two countries when the country outside the European Union is covered by an adequacy decision confirming that it offers an adequate level of protection for personal information.

He believes that it would be easier to convince young people, the heaviest users of social media platforms, about the importance of taking privacy issues seriously if these laws were applicable to government conduct and the conduct of political parties.

Considering the above, the Committee makes the following recommendations.

Recommendation 2

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* to impose additional data minimization obligations on organizations subject to the Act, including a ban on engaging in certain forms of data collection.

Recommendation 3

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* to give the Privacy Commissioner of Canada the power to make binding orders and impose significant administrative monetary penalties.

Recommendation 4

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* to include explicit rules surrounding the transfer of Canadians' personal data outside the country to ensure equivalent levels of protection for data transferred outside of Canada.

Protecting the Privacy of Minors

On protecting the privacy of minors online, Mr. Dufresne had this to say:

> Growing up in the digital age presents significant new challenges for the privacy of young people. As children and youth embrace new technologies and experience much of their lives online, we need strong safeguards to protect their personal information, and how it may be collected, used and disclosed. Increasingly, their information is being used to create personalized content and advertising profiles that are ultimately aimed at influencing their behaviours.
>
> Children have a right to be children, even in the digital world. As UNICEF notes in its policy guidance on artificial intelligence for children, young people are affected by digital technologies to a greater extent than adults. Young people are also less able to understand and appreciate the long-term implications of consenting to their data collection. Privacy laws should recognize the rights of the child and the right to be a

> child. This means interpreting the privacy provisions in the legislation in a way that is consistent with the best interests of the child.

Mr. Dufresne said that it is vitally important that government and organizations take action to ensure that young people can benefit from technology and be active online without the risk of being targeted, manipulated or harmed as a result. He referred to the joint declaration on the best interests of children that he and his provincial and territorial colleagues issued in August 2023. It sets out the privacy commissioners' expectations and includes recommendations.[91] The joint declaration also includes recommendations about making sure that organizations are protecting children and the best interests of the child and that they are treating their information appropriately.

The commissioners' recommendations include the following: provide privacy tools and consent mechanisms appropriate for young people and their maturity level; reject deceptive practices that influence young people to make poor privacy decisions or to engage in harmful behaviours; and allow for deletion or deindexing of information collected when the users were children.[92]

Mr. Dufresne added that the OPC made a number of recommendations to ban online nudging behavioural techniques. He said that studies show how social media is addictive for children. Sometimes the social media business model is to try to encourage them to stay longer, because that is what generates more revenues.

Dr. Laidlaw referred to some of the social media platform practices involving children as mind manipulation. She believes that interventions similar to those made in the advertising industry in the past to prevent certain ads from being broadcast at certain times of the day or during children's programs should be taken to protect children online.

However, in answer to questions about Meta's impact on minors, Ms. Curran said that "the most recent research that we have doesn't support the hypothesis that digital technology is behind trends in teen mental health and well-being." She said that other factors such as economic instability and substance use are behind trends in teen mental health and well-being.[93] She also said that it would be "wrong and even irresponsible to suggest that a single factor is the cause of trends in teen mental health."

---

91 OPC, *Putting best interests of young people at the forefront of privacy and access to personal information*, October 2023.

92 Ibid.; ETHI, *Evidence*, Dufresne.

93 See also: ETHI, *Evidence*, Curran.

Regarding Bill C-27, Mr. Dufresne said that he is encouraged by statements from the Minister of Innovation, Science and Industry indicating that the government is prepared to amend the bill in order to strengthen children's privacy rights, adding in its preamble that the processing of personal data must protect the best interests of the child.[94] However, Mr. Caraway added that the protection of children must be included in the bill's provisions and not just in its preamble.

Mr. Dufresne also said greater obligations in terms of care and methods of consent are required for minors, given that their personal information is considered sensitive. He said that the OPC guidelines for obtaining meaningful consent under PIPEDA specify that parental consent should be required under certain circumstances, including for any children 13 and under.[95]

PIPEDA contains no specific obligation concerning the personal information of minors. The CPPA provides that any personal information of minors is to be considered sensitive information[96]

The PACC would define the term "minor" in the CPPA as someone under the age of 14 in order to align with the Quebec legislation, which requires parental consent to collect personal information on an individual under 14 years of age.[97] An amendment adopted by the parliamentary committee reviewing Bill C-27 has added the following definition of the term minor in the CPPA: "an individual under 18 years of age."[98]

Another important right for minors, according to Mr. Dufresne, is the right to disposal found in section 55 of the CPPA:

> When I say that children have a right to be children, that's what I'm alluding to. Children do things online. If it stays online forever, then they're treated as adults right from when they're teenagers. It stays forever, and it could be used against them for jobs and so on and so forth.

Regarding the possibility of requiring an online age verification mechanism, Mr. Dufresne said that the OPC's position is that age verification tools need to be appropriate and not ask for too much personal information. Age verification also needs to be context-

94 See: INDU, *Correspondence from the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry*, 3 October 2023.

95 OPC, *Guidelines for obtaining meaningful consent*, 13 August 2021.

96 Bill C-27, CPPA, para. 2(2).

97 PACC, *Brief*, p. 22, Recommendation 21.

98 House of Commons, Standing Committee on Industry and Technology, *Minutes*, 29 April 2024.

appropriate. Some websites may be higher risk and require tighter verification. Others may be aimed at children.

Ms. Polsky also expressed concerns about this practice. The PACC believes that online age verification requires the disclosure and collection of sensitive personal information, which is inconsistent with Bill C-27's objective of protecting minors.[99] It noted, for example, that such a requirement is found in Bill S-210, An Act to restrict young persons' online access to sexually explicit material. Although the bill includes an obligation to destroy personal information collected once age verification has been completed, the PACC believes that there is nothing guaranteeing that this requirement will be met.[100]

Regarding the possibility of using age detection technology and age verification, Mr. Lieber said that while they can be helpful in more accurately determining users' ages, they also have privacy implications.

As to whether it would be appropriate to require parental consent for any individuals under the age of 16 to be able to download a social media app, Mr. Larkin was not opposed to the idea. Mr. Andrey said that while such a requirement would probably not be harmful, the logistics around age verification are tricky. Mr. Malone had an opposing view. He said that requiring parental consent to download apps would have adverse effects. In his view, this should not be the responsibility of a parent. Instead, what is needed is privacy legislation that protects children by default.

Mr. Fernandez did not take a formal position on requiring parental controls over the downloading of social media apps by teens. He pointed out that X is not the platform of choice for teens. Ms. Curran said that Meta would support this kind of restriction, as long as it is applied industry-wide. Ms. Patell said that parental controls can be put on Android devices, which can restrict what can be downloaded from Google Play based on age.

Considering the above and the importance it places on online privacy for minors, the Committee makes the following recommendations.

---

99 Bill S-210, An Act to restrict young persons' online access to sexually explicit material.

100 PACC, *Brief*, paras. 40, 83, 104–106; Bill S-210, An Act to restrict young persons' online access to sexually explicit material. At the time of the adoption of the report, the bill was at the third reading stage in the House of Commons.

Recommendation 5

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* to require organizations subject to the Act to provide consent mechanisms appropriate for minors and include an explicit right in the Act to the deletion or deindexing of the personal information of minors.

Countering Disinformation, Misinformation and Harmful Content Online

Disinformation and Misinformation

To fight against disinformation, Dr. Gruzd recommended a comprehensive approach that would compel platforms to do three things. Platforms should: adopt the principles of privacy by design and by default; invest in expanding their trust and safety teams; and share data with researchers and journalists.

Dr. Gruzd told the Committee that while individual education is one of the ways to fight disinformation and misinformation, platforms should be compelled to incorporate tools that can signal whether something is potentially problematic. He gave the example of COVID-19, when platforms stepped up and provided useful interventions, such as adding a link to Health Canada when somebody talked about COVID-19 or flagging that some of the content in the post may not accurately relate to scientific knowledge. He believes that those interventions are helpful in reducing the spread of misinformation.

Dr. Laidlaw recognized that finding solutions is particularly challenging when it comes to misinformation and disinformation because, "except in narrow circumstances, it is lawful to believe and share false information."

To evaluate how well platforms are combatting disinformation, Dr. Gruzd also recommended that Canada create a EU-style code of practice on disinformation and a transparency repository that would require large platforms to report regularly on their trust and safety activities in Canada.[101] For example, he said that under the EU *Digital Services Act*, platforms with more than 45 million users must report on their activities and what they have done to stop foreign interference, country by country, about every

101 European Commission, 2022 Strengthened Code of Practice on Disinformation, 16 June 2022; ETHI, *Evidence*, Gruzd. These are self-regulatory standards for the industry.

six months. They must also report on what steps they have taken to combat disinformation.[102]

To increase transparency and oversight, Dr. Gruzd also recommended that Canada mandate data access for researchers and journalists. He believes that this access is essential to independently detect harmful trends. He said that in the EU, this is achieved through the new *Digital Services Act*.[103] He said that TikTok does not provide data access to Canadian researchers, but it does so for those who reside in the U.S. and EU. He said that X recently shut down its free data access for researchers.[104] However, Mr. Fernández said that X has

> an open public [Application Program Interface], making data available for developers, journalists, brands and researchers for analysis, and to build businesses, provide services and create innovative products.

Dr. Gruzd also recommended that content moderation teams be expanded. He noted that trust and safety departments appear to be shrinking. He believes that having fewer trust and safety teams can affect the proliferation of harmful content online.

Considering the above, the Committee makes the following recommendation.

Recommendation 6

That the Government of Canada adopt an European Union-style code of practice on disinformation and compel social media platforms to report regularly on their trust and safety activities in Canada and to provide Canadian researchers with access to their data.

Legislative Framework Regarding Online Harms

In 2021, the government promised to put in place a transparent and accountable regulatory framework for online safety in Canada.[105] The discussion guide for the online consultation that took place that same year listed five categories of harmful content targeted by this proposed legislative framework: terrorist content; content that incites

102 ETHI, *Evidence*, Gruzd; European Union, *Official Journal of the European Union*, Digital Services Act.

103 Ibid., art. 40.

104 ETHI, *Evidence*, Gruzd.

105 Government of Canada, *The Government's commitment to address online safety*.

violence; hate speech; non-consensual sharing of intimate images; and child sexual exploitation content.[106]

Roundtables on online safety and a citizens' assembly on democratic expression took place in 2022. That same year, an expert advisory group on online safety was established to provide the Minister of Canadian Heritage with advice on how to design a legislative and regulatory framework to address harmful content online.[107]

On February 26, 2024, the Government of Canada introduced Bill C-63, An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts. According to its summary, among other objectives of the bill, part 1:

> [E]nacts the *Online Harms Act*, whose purpose is to, among other things, promote the online safety of persons in Canada, reduce harms caused to persons in Canada as a result of harmful content online and ensure that the operators of social media services in respect of which that Act applies are transparent and accountable with respect to their duties under that Act.

Bill C-63, if adopted in its current form, could address some of the issues identified by the witnesses.

Access to harmful content can have negative consequences. For example, Ms. Henderson said that some young people go onto these social media platforms and then can get into some extremist milieu and get very influenced in a negative way. She explained that terrorist organizations in other countries monitor social media, create websites and try to lure vulnerable youth.

Dr. Laidlaw said that the health of our information economy now depends on privately owned digital platforms and the choices they make in the design of their products, corporate governance and culture, and content moderation systems. She told the Committee that Canada is lagging behind when it comes to regulating social media platforms, since it has not yet passed online harms legislation. Such legislation is already in place in Europe, the U.K. and Australia. Canada can learn from other legislation in force. She believes that Canada needs to pass online harms legislation before we see more coordinated global investigations.

106 Government of Canada, The Government's commitment to address online safety, *Discussion guide*.

107 Government of Canada, *The Government's commitment to address online safety*.

Mr. Andrey added that Canada can learn from other countries' mistakes. He pointed to Germany, which created a 24-hour takedown regime, which resulted in over-censorship. Social media platforms, not wanting to be held liable, removed legal content. The legislation has since been amended.[108]

Dr. Laidlaw explained the risks of passing inadequate legislation.

> If you pass a law that just incentivizes a focus on harms, you incentivize companies to put in rudimentary solutions that, in fact, backfire. There's been a lot of evidence of backfiring, where what ends up being silenced is racialized and other marginalized voices.

Therefore, in her view, social media platforms that care about harms need a dual focus: protecting and promoting freedom of expression; and the ability to demonstrate to a regulator the steps they are taking to remove harmful content and prove that these measures are contextual and adapted to their services.

Dr. Laidlaw also explained why a legislative framework for social media platforms is important and how such a framework needs to be designed. First, platform regulation is a field like protecting the environment, and multiple areas of law must work in concert to protect our safety and rights. Privacy law and online harms legislation are mutually reinforcing, so both are needed.[109] She gave this explanation:

> Algorithms that push harmful content do so by harvesting personally identifiable information, which is covered by privacy law. However, the algorithm can also draw from anonymized aggregate data, which falls outside of privacy law.

Dr. Laidlaw also said that Bill C-27, which is based on a consent paradigm, does not address some of the more problematic aspects of social media and their influence, which, really, nobody can consent to. Therefore, Canada also needs online harms legislation that targets the choices social media platforms make in product designs and content moderation systems.[110]

Second, social media platforms can be important collaborators and innovators in solving problems. They must be part of the solution. Dr. Laidlaw did acknowledge there is some friction when a platform is almost state-like in its role, for instance when it has its own

---

108 See, for example: United States, Library of Congress, *Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech*.

109 ETHI, *Evidence*, Emily Laidlaw (Associate Professor and Canada Research Chair in Cybersecurity Law, University of Calgary).

110 ETHI, *Evidence*, Laidlaw.

national security team that essentially sets policies in this area. Other platforms, alternatively, do very little to manage the risks associated with their products. Therefore, while it is critical to have social media platforms engaged in addressing hateful content, disinformation and violent extremism, Dr. Laidlaw believes that this involvement is not a substitute for law to set industry standards.

Third, Dr. Laidlaw told the Committee that the risks of harm are not the same for all types of harmful content. She said that child protection, hate and terrorist propaganda, disinformation and violence all have different dynamics and should not be distilled into one legal rule, except for the basic idea of corporate due diligence. This type of content creates risks for fundamental rights such as the right to freedom of expression, the right to privacy and the right to equality.

Dr. Laidlaw summarized the basic components needed for online harms legislation. First, such legislation should require social media platforms to manage the risks of harm of their products and to protect fundamental rights. Then, it should impose transparency obligations matched with a way to enable vetted researchers to conduct audits and access data. A regulator to investigate companies and educate the public should also be created. Lastly, the legislation should allow victims to access recourse, given that harms can be both collective and individual.

Dr. Laidlaw remarked that transparency on its own is meaningless. She believes that an avenue to investigate, audit and lift the lid on these companies proactively is required. Mr. Caraway also noted the importance of a third-party audit of how data is used by a digital platform.

As for a regulator responsible for online harms legislation, Dr. Laidlaw said that a regulator could be more agile than the courts.[111] She recommended that the regulator have the power to investigate companies and to audit companies for their compliance with specific duties. She said that this regulator should be independent from government and be able to impose hefty monetary penalties.

Mr. Andrey in turn recommended that the online harms regulator be the same one created by Bill C-27 in Part 3, the Artificial Intelligence and Data Act (AIDA). Like Dr. Laidlaw, he insisted that the regulator be independent from Innovation, Science and Economic Development Canada (ISED).

111 ETHI, *Evidence*, Laidlaw.

According to Dr. Laidlaw, the online safety regulator should also play a significant public education role, like Australia's eSafety Commissioner.[112] While recognizing that education is a provincial responsibility, she said that a federal curriculum could be developed and shared with the provinces to influence curricula in schools and even municipalities.

Governing the Use of Artificial Intelligence

Bill C-27 creates the Artificial Intelligence and Data Act (AIDA), which is designed:

- to regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of those systems; and

- to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests.

Dr. Laidlaw said that as currently worded, the AIDA is not sufficiently developed to be able to actually cope with the problems involving AI. She believes that it needs to be carved out from the bill so that there can be a proper discussion about the ways in which AI can be used that will fundamentally disrupt democracy, interfere with our ability to make decisions and create physical risks to us individually or collectively.

Mr. Malone was critical of the fact that the AIDA does not apply to the government and that it falls under the responsibility of a commissioner who is not entirely independent of ISED, whose mandate is to grow the economy.

More generally, Dr. Gruzd explained that in light of developments in generative AI, tools need to be found so that individual users can detect what is real and authentic on platforms, for example through digital certification or by requiring content creators to disclose whether any generative AI tools were used to produce content.[113] He also pointed out the need to know whether Canadian data is being used to train generative AI applications and whether this content is generated by AI or not. For example, he pointed out that Canadian users are providing personal information to websites with

112 ETHI, *Evidence*, Laidlaw; Australia, eSafety Commissioner, eSafetyeducation.

113 ETHI, *Evidence*, Gruzd.

generative AI tools such as ChatGPT without realizing that they are actually consenting to that data being used for future training of the app.

Dr. Gruzd said that machine learning in AI is heavily used to "deliver content to eyeballs." This sometimes leads individuals into echo chambers that could be full of misinformation, driven by a recommended system. In his view, any unregulated use of AI can be misused in the future.

Dr. Gruzd also raised concerns about the use of AI to detect harmful online content. He noted, for example, that according to transparency reports from Meta, the company automatically removes 65% of the content that was classified as harassment and bullying. For the remaining 35%, users had to report the content in order for the platforms to act.

In its written response, the RCMP states that, from a law enforcement perspective, AI could be a new avenue for investigative tools, especially in data-rich and complex investigations.[114] The RCMP states that it

> assesses, as various new technologies become available, the use of AI as an investigative tool for law enforcement to augment and support traditional policing investigative tactics and ensuring that its use is done in a responsible, transparent, and lawful manner. There are, however, risks to the use of AI, including in particular the potential for bias to be introduced or exacerbated. As such, the RCMP acknowledges the need for the development of policies and procedures and training to guide the adoption and use of AI technology in a law enforcement environment to ensure its use addresses all legal and privacy concerns.[115]

Regarding the possibility of establishing a national registry of all AI applications or their use by social media platforms, Mr. Larkin was open to discussing it without commenting on the value of such a registry. Ms. Luelo did not give an opinion on such a registry. She did say that internally, guidance provided inside government is to ensure transparency around the use of AI, including generative AI.[116]

---

114 Royal Canadian Mounted Police, *Written response submitted to ETHI*, p. 2 [HYPERLINK NOT AVAILABLE]. See also: ETHI, *Evidence*, Brigitte Gauvin (Acting Assistant Commissioner, Federal Policing, National Security, Royal Canadian Mounted Police).

115 Ibid.

116 See for example: Government of Canada, *Guide on the use of Generative AI*.

CHAPTER 4: PROMOTING SAFE USE OF SOCIAL MEDIA PLATFORMS

Education and Awareness for Canadians

Mr. Dufresne said he hoped that the OPC would do more in terms of educating Canadians about privacy issues. He did note that this is a collective effort for government, schools and teachers. Ms. Polsky agreed that education is important. She said that few people, even those knowledgeable about privacy, understand the extent to which personal information can be shared online.

Mr. Khoury said that CSE publishes guidance through its CCCS. These resources help Canadians make informed decisions about the online services they use. For example, the CCCS recommends researching the app or platform to determine whether it is trustworthy and reading the terms of use and conditions. It also recommends finding out where the data collected by an app is hosted and what privacy impact this could have.[117]

Ms. Henderson agreed. She said that any Canadian creating a social media account needs to know where the account is being created. She also spoke about how important it is to educate people on good social media hygiene. She believes that everyone must take responsibility for what they are sharing and is aware of the cost and the impact that could have on them.[118]

Ms. Henderson added that with the advent of social media and technology, Canadians are being exposed to the activities of hostile states interested in undermining Canada's sovereignty and democratic institutions. This makes it fundamentally important to protect national security, including "with awareness and education, in order to protect ourselves and our systems moving forward." She believes that protecting Canada's national security requires a whole-of-society effort, including communities, academia and governments at all levels.

Ms. Gauvin also said that education is useful for countering foreign interference on social media platforms. People need to be aware that they can be monitored by foreign entities online. That is why the RCMP has "engagement programs with the public, private entities and more vulnerable communities to educate people about the different

117 ETHI, *Evidence*, Khoury.

118 ETHI, *Evidence*, Henderson.

ways or various mechanisms used by foreign entities to engage in interference activities."

Mr. Larkin explained that the RCMP's National Cybercrime Coordination Centre and the Anti-Fraud Centre are engaged in the "Get Cyber Safe" online safety public awareness campaign.[119] This national campaign aims to inform all Canadians, including youth, about cyber-threats and prevention. The RCMP also produces operational bulletins and reporting tools for frontline police officers, strategic partners and the public. The goal is to increase the reporting on federal crimes and engage with culturally diverse communities. The National Child Exploitation Crime Centre conducts awareness campaigns focused on protecting vulnerable individuals.[120]

Mr. Larkin acknowledged that it is challenging for the RCMP to react to the impact of social media. This means that much of the RCMP's work is reactive in nature. He also remarked that the RCMP's capacity is limited.

Mr. Malone said that the cybersecurity resources available to the RCMP are not meeting the demand and that it is underfunded. He pointed out that in 2018, Public Safety went through a cybersecurity update and provided new funding to the RCMP to fight cybercrime, announcing the creation of NC3, the national cybercrime coordination centre. He noted that the reporting system is two years behind schedule and that the website is still in beta testing and accepts only 25 cybercrime complaints a day for the entire country.[121]

Mr. Malone added that the number of people working for the government in social media or communications is exponentially larger than the resources and personnel that the RCMP is devoting to fighting online harms. For example, he said that the RCMP's cybercrime investigative team has only eight employees in all of Alberta, four employees in all of British Columbia and none in Saskatchewan, Manitoba or any of the maritime provinces.[122]

Dr. Gruzd said that while teaching digital literacy is important, it is unfair to place all the responsibility on individuals. Social media platforms are complex, and the algorithms that decide what users see and do not see remain black boxes. Strategies that compel

119 Government of Canada, Get Cyber Safe.

120 ETHI, *Evidence*, Larkin.

121 RCMP, *The National Cybercrime Coordination Centre (NC3)*; RCMP, *New cybercrime and fraud reporting system*.

122 ETHI, *Evidence*, Matt Malone (Assistant Professor of Law, Thompson Rivers University).

companies to implement privacy by design and by default are therefore needed. He added that while it may be hard to train each user and change individual behaviour, platforms can incorporate tools that can help users protect themselves more efficiently and effectively.

Education and Awareness for Minors

Mr. Dufresne would hope to see mandatory training in schools early on, so that individuals can get the tools early on. Ms. Polsky added that there should be a way to include digital literacy in school curricula across Canada, while recognizing that education falls under provincial jurisdiction.

Dr. Gruzd said that there must be interesting ways of educating teens and young adults, for example through games where players have to manage an online information operation, allowing them to become more aware of everything that can happen to them in their online interactions.

Ms. Henderson and Mr. Khoury also agreed that education is needed for everyone, including young people. Mr. Khoury said it is important to keep both young people and not so young people informed of the risks that posting certain information online could have in the future, once a more complete portrait or profile of the individual has been compiled. Ms. Polsky gave the example of questions asked through online quizzes, which are subtle ways of gathering information about individuals, including their psychological makeup and preferences, for future use.

Mr. Larkin acknowledged that youth are particularly vulnerable to cybercrime, as they tend to trust in the digital environment without fully grasping the risks. “Their extensive use of social media platforms coupled with the tendency to overshare personal information makes them particularly attractive targets for cybercriminals.” That is why the RCMP’s national youth services are engaged and educate young people about online safety through collaboration with school resource officers and various organizations.

Considering the importance of educating Canadians and making them aware of online safety and the RCMP’s role in fighting cybercrime, the Committee makes the following recommendations.

Recommendation 7

That the Government of Canada increase funding to the Royal Canadian Mounted Police so additional resources can be allocated to providing education and to fighting cybercrime.

Recommendation 8

That the Government of Canada invest more in digital literacy to better equip Canadians to protect their personal information online, recognize disinformation and misinformation, and identify harmful content online.

CONCLUSION

This study allowed the Committee to confirm that the business model and practices of social media platforms pose certain risks to the health and safety of their users—and even the general population—and to Canada's national security. These risks should be mitigated for example by modernizing federal privacy legislation so that it governs data transfers and takes into account technological advancements such as artificial intelligence.

Bill C-27 could address some of the issues with the current legislative framework identified by the witnesses, although the content of its final provisions, if adopted, is not yet known.

The Committee is also particularly concerned by the health and safety of the children who use social media and believes that it is vital that they be protected in their online activities. The Committee, as the Privacy Commissioner aptly put it during the study, firmly believes that children have a right to be children, even in the digital world.

Lastly, the Committee firmly believes that more work is needed to address the digital literacy of Canadians and that the capacity of law enforcement to fight cybercrime and foreign interference must be substantially expanded. As the Committee has already stated in past studies, the self-regulation of social media platforms is insufficient to protect the health and safety of their users and Canadians in general. The Committee considers that now, more than ever, a more stringent legislative framework for social media platform oversight is needed.

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
TikTok	2023/10/18	85
Steve de Eyre, Director Public Policy and Government Affairs, Canada		
David Lieber, Head, Privacy Public Policy for the Americas		
Offices of the Information and Privacy Commissioners of Canada	2023/10/25	87
Philippe Dufresne, Privacy Commissioner of Canada		
Michael Maguire, Director, Personal Information Protection and Electronic Documents Act, Compliance Directorate		
Canadian Security Intelligence Service	2023/11/20	92
Cherie Henderson, Assistant Director, Requirements		
Peter Madou, Director General, Intelligence Assessments		
Communications Security Establishment	2023/11/20	92
Sami Khoury, Head, Canadian Centre for Cyber Security		
Privacy and Access Council of Canada	2023/11/20	92
Sharon Polsky, President		
As an individual	2023/11/27	94
Anatoliy Gruzd, Professor and Canada Research Chair in Privacy-Preserving Digital Technologies, Toronto Metropolitan University		
Royal Canadian Mounted Police	2023/11/27	94
Brigitte Gauvin, Acting Assistant Commissioner, Federal Policing, National Security		
Bryan Larkin, Deputy Commissioner, Specialized Policing Services		

Organizations and Individuals	Date	Meeting
Treasury Board Secretariat	2023/11/27	94
Catherine Luelo, Deputy Minister and Chief Information Officer of Canada		
As an individual	2023/12/04	95
Brett Caraway, Associate Professor of Media Economics, University of Toronto		
Emily Laidlaw, Associate Professor and Canada Research Chair in Cybersecurity Law, University of Calgary		
Matt Malone, Assistant Professor, Thompson Rivers University		
The Dais	2023/12/04	95
Sam Andrey, Managing Director		
Joe Masoodi, Senior Policy Analyst		
Google Canada	2023/12/13	97
Shane Huntley, Senior Director, Threat Analysis Group, Google		
Jeanette Patell, Head of Canada Government Affairs and Public Policy, Google and YouTube		
Meta Platforms Inc.	2023/12/13	97
Rachel Curran, Head of Public Policy, Canada		
Nathaniel Gleicher, Head of Security Policy		
Lindsay Hundley, Influence Operations Policy Lead		
X Corporation	2023/12/13	97
Wifredo Fernández, Head of Government Affairs, United States of America and Canada		
Josh Harris, Senior Privacy and Data Protection Counsel		

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.

Privacy and Access Council of Canada

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. 85, 87, 92, 94, 95, 97, 106 and 137) is tabled.

Respectfully submitted,

John Brassard
Chair