HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 124 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, November 1, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, November 1, 2018

● (1130)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Welcome, everyone, to the Standing Committee on Access to Information, Privacy and Ethics, meeting number 124. Pursuant to Standing Order 108(3)(h)(vii), we are studying a breach of personal information involving Cambridge Analytica and Facebook.

Today we have two sections. Each will be about 45 minutes, slightly shortened based on the votes we just had. From Elections Canada, we have Stéphane Perrault, Chief Electoral Officer; and Anne Lawson, deputy chief electoral officer, regulatory affairs.

From the CRTC, the Canadian Radio-television and Telecommunications Commission, we have Rachelle Frenette, legal counsel; Scott Hutton, executive director, broadcasting; and Neil Barratt, director, electronic commerce enforcement. We'll start with Mr. Perrault.

Go ahead.

Mr. Stéphane Perrault (Chief Electoral Officer, Elections Canada): Thank you, Mr. Chair.

In the interest of time, I will use a slightly truncated version of my speech. If you see me skipping paragraphs, it's to save time.

[*Translation*]

Thank you for the opportunity to speak with the Committee today.

Today I would like to address four subjects that have drawn Elections Canada's close attention and that relates to your study: foreign interference, the digital information environment, cybersecurity and privacy.

I am grateful for this opportunity to explain to the Committee what role Elections Canada is playing to preserve trust in our electoral process, and to outline where we are collaborating with others, on the understanding that no single solution and no agency working alone can address these threats.

Let me first start with the issue of foreign interference, which overlaps in part with the other topics that I have identified.

In Canada, recent concerns about foreign interference have been primarily around issues of foreign funding of third parties—entities that seek to influence the electoral debate without participating directly as parties or candidates.

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

As you are aware, foreign interference can take other forms, including disinformation campaigns and cyberattacks.

The expansion of the web and social media has transformed our information environment. Citizens are no longer simply struggling to determine who is a journalist; they are unlikely to know whether a given social media post or ad was sent by a bot or a human, or whether it is a genuine expression of belief or part of an influence campaign, domestic or foreign.

There is no simple solution to this, but elements of a response are emerging. Efforts to increase digital literacy are, in my view, a key element. It is reassuring to know that Canadians are increasingly cautious about what they see or read on social media. I would add that they generally trust the conventional media.

Bill C-76 would include a requirement for social media platforms to publish and preserve archives of election and partisan ads. This is a positive step that supports transparency and aids enforcement.

Bill C-76 would also clarify and expand existing provisions against some kinds of online impersonation, as well as false statements about candidates.

● (1135)

[*English*]

Elections Canada's specific and essential role is to ensure that Canadians have easy access to accurate information about the voting process, including information about where, when and how to register and to vote.

In preparation for the next election, we plan to launch a voter information campaign starting next spring. We will also be monitoring the social media environment throughout the election period, which will enable us to rapidly correct any inaccurate information about the voting process. And we will create an online repository of all of our public communications, so that citizens and journalists can verify whether information that appears to be coming from Elections Canada actually is. This is something that I have encouraged political parties to consider doing regarding their own communications, to have a central repository of their communications.

Together with the Commissioner of Canada Elections, we have also engaged representatives from social media platforms to better understand how they operate and to establish channels of communication to rapidly respond to incidents during the election.

A third area of concern is cybersecurity. While we continue to rely on hand-counted paper ballots, Elections Canada is increasingly delivering online services to voters, the candidates and the parties. One of my key responsibilities is to protect Elections Canada's digital assets, based on the advice and expertise of our federal security partners.

Over the last two years, we have made significant investments to renew our IT infrastructure and to improve our security posture and practices. As part of this effort, we are also providing security awareness training to staff at headquarters and to all 338 returning officers in the field.

Other participants in the electoral process, including media and parties, must also protect themselves against hacking. The Canadian Centre for Cyber Security offers excellent resources and advice to everyone. Some measures are inexpensive and can be quite effective. Other measures, however, may require considerable investments.

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

The last point I want to address is the issue of privacy. This committee has recommended that political parties be made subject to basic privacy rules and oversight by the Privacy Commissioner of Canada. This is a recommendation that I also support and have made in the context of Bill C-76. I was disappointed that it was not accepted at committee.

Parties, as you know, increasingly rely on voter data to support fundraising and campaigning activities. This data may include, in addition to the information that we provide to parties and candidates, information about a person's political affiliation or support, volunteer activities, or other information that the party believes to be relevant to its purposes.

Bill C-76 would require parties to publish their own privacy policy. This is a small step in the right direction, as the bill provides no minimal standards and no oversight.

Bill C-76 is also silent on whether a party's policy should include a mechanism allowing Canadians to validate and correct any information that the parties hold on them. Of course, nothing prevents parties from doing so, or from taking other steps to reassure Canadians about the collection, use and protection of their information.

It has been observed that parties have much to gain in having robust privacy policies and practices, and I believe that to be the case. Above all, more importantly, I believe that electoral democracy has much to gain.

Mr. Chair, I would like to conclude by emphasizing the importance of the work undertaken by the committee. I would be happy to answer any questions the members may have.

Thank you.

The Chair: Thank you, Mr. Perrault.

Next up we'll have Mr. Hutton, for 10 minutes.

Mr. Scott Hutton (Executive Director, Broadcasting, Canadian Radio-television and Telecommunications Commission): Thank you, Mr. Chair, for this opportunity to participate in the committee's valuable examination of how to better protect the private data of Canadians.

I will spare you the introductions, to save a bit of time.

As the committee members know, the CRTC derives its mandate from various pieces of legislation. The Broadcasting Act authorizes the CRTC to regulate the industry in pursuit of specific objectives, including to encourage the creation and promotion of content made by Canadians and that reflects Canadians in all their facets.

● (1140)

[*Translation*]

Similarly, the Telecommunications Act assigns the CRTC the mandate to regulate the telecommunications industry in pursuit of particular goals. For instance, ensuring that Canadians in urban and rural areas have access to reliable, affordable and high-quality telecommunications services.

The Telecommunications Act also gives the CRTC the authority to regulate unsolicited telecommunications and to take enforcement action against non-compliant telemarketers.

For its part, Canada’s anti-spam legislation authorizes the CRTC to regulate specific types of electronic communications. These include the transmission of commercial electronic messages, the alteration of transmission data in electronic messages and the installation of programs on another person’s computer system.

Of course, the CRTC, like all other federal departments and agencies, abides by Canada’s Privacy Act.

Moreover, the Telecommunications Act requires that the telecommunications sector contribute to the protection of the privacy of individuals. The CRTC’s policies in this area are limited to the protection of confidential consumer information held by telecommunications service providers.

[*English*]

The CRTC appreciates the committee's work on digital platforms. Earlier this year, we published a report titled “Harnessing Change: The Future of Programming Distribution in Canada”. The report's perspective is informed by CRTC's mandate, of course. As such, much of the report focuses on the creation, distribution and promotion of Canadian audiovisual content.

In a digital age, users can now access a growing wealth of content and platforms. As a result, the traditional regulatory approach is less and less able to obtain the objectives set out in legislation such as the Broadcasting Act. To address this reality, the report suggests innovative approaches to policy and regulation, approaches that would engage digital platforms that provide audiovisual content to Canadians.

[*Translation*]

We proposed that three principles should guide any new approaches.

First, future policy approaches should not only focus on the production and promotion of high-quality content made by Canadians, but also on its discoverability.

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

And finally, future legislation and regulation must be nimble and capable of easily adapting to ever-changing consumer behaviour and technologies.

The report also identifies some of the opportunities created by the evolution of digital technologies. For example, data on how people find, select and interact with content could inform how to develop and distribute content in ways that support Canada’s broader policy objectives.

[*English*]

That being said, we recognize that digital communications technologies pose particular risks to the protection of personal information. The report describes the problem as follows:

> The development of these online services has also given rise to new ways of misusing data—for example, to infringe on the privacy of Canadians—particularly when services collect data without users’ knowledge or informed consent. Data can also be used to misinform and manipulate through fake [news] or misleading news and information, affecting democratic processes, relationships with others and the way Canadians view the world.

The CRTC firmly believes that protecting the personal data of Canadians and preventing abuses must remain the overriding consideration. The legislative and regulatory frameworks that govern the protection of privacy and the use of personal data, however, are not part of CRTC's mandate on the broadcasting side.

Thank you.

We'll do our best to answer your questions.

● (1145)

The Chair: Thank you, Mr. Hutton.

We'll go to the first round, beginning with Ms. Vandenbeld for seven minutes.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much.

Most of my questions will be for Elections Canada and Mr. Perrault. Considering that I was on PROC when we were reviewing the Chief Electoral Officer's recommendations after the last election, this is an area of significant interest to me, as I think it is to all members of this committee.

You testified before PROC, and again in your remarks this morning, that political parties should come under privacy rules. Now, PIPEDA, of course, is where commercial entities fall. The Elections Act is another potential tool that could be used. We've heard testimony before this committee that there's a need to ensure that political parties can access voters without interference, that they're different, and that for political campaigns, for instance, the do-not-call list doesn't apply. You can enter apartment buildings during campaigns so that you can reach all voters.

Are there specific, unique qualities of an election campaign such that you think the regular PIPEDA rules would not apply to political parties? Would it be better for us to do this under the Elections Act or under PIPEDA?

Mr. Stéphane Perrault: There are a lot of elements in that.

I do think parties should have access to information that allows them to reach out to voters. That's a fundamental aspect of our system, and that should remain.

I do think we have now reached a point where concerns over the use of personal data on the Internet require some measure of protection and some minimal standards. Whether they be in the Elections Act or the other pieces of legislation, I do think this is an area of expertise for the Privacy Commissioner. My preference is that it be under his area of jurisdiction.

I also recognize that there are unique realities to parties. I think the basic principles of privacy can accommodate those realities. If you look at areas of consent and how you obtain consent—i.e., whether it has to be prior consent or the right of a person to seek to erase information rather than give up-front consent—these are areas where the principles, I believe, allow for some flexibility, but I do not believe there should be no minimum standards applicable to parties. That to me is a basic element. There should be some form of oversight.

Ms. Anita Vandenbeld: Of course, one thing we've been concerned about on this committee is the data breach and Cambridge Analytica. There are third party entities that are global in nature and that are gathering huge amounts of data. This allows for very specific targeting of people who are on social media platforms, which has, as we've seen, influenced different campaigns.

Beyond the things you were talking about in terms of third parties and voter awareness, is there a role for Elections Canada in monitoring the kind of targeting that is happening on Facebook? For instance, let's say a third party entity that is not spending money—they may be a foreign source or they may be domestic—is targeting particular groups of voters for voter suppression. An ad goes to, for instance, young men between 20 and 25 who are of a particular racial minority. It tries to get people not to vote.

Is there a role for Elections Canada, or in the Elections Act, even legislatively, to be able to prevent that kind of voter suppression?

Mr. Stéphane Perrault: Again, this is not a simple area. The premise, at least in organic content, is that we don't regulate what's being said. There are exceptions to that in the legislation. There are exceptions in Bill C-76, such as when there is specific impersonation, for example. There are areas of legitimate intervention. If we see offences under the act, we will report them to the commissioner. He's the one to enforce that.

We do have an Elections Canada electoral integrity office. We've had that now for two cycles. That office is concerned with looking at malpractices that emerge in other jurisdictions to see whether there may be trends, to be prepared to at least alert either the commissioner or the person who may be caught in those situations and to react.

Our basic role is really to make sure that people have correct information about the voting process. Really, that's the core of our mandate, and that's where we have to focus our attention.

Ms. Anita Vandenbeld: We know that this is not a uniquely Canadian problem. This is something that is happening around the world. Is Elections Canada working with other electoral bodies around the world to look at best practices, at how other bodies are handling this or at how to coordinate in responding to those that are across boundaries?

● (1150)

Mr. Stéphane Perrault: We certainly have regular exchanges with other electoral management bodies, both in Canada and in other jurisdictions. I think it's fair to say that nobody has found a silver bullet to deal with these issues, but we are looking at similar approaches.

Ms. Anita Vandenbeld: I'd like to go back to the actual cybersecurity of the Elections Canada voters list. We have heard in this committee that it isn't necessarily the actual institutions, Elections Canada, or the process of voting...particularly with the paper ballots, which is something that I think we want to keep as a country so that we have the manual counting of ballots. At the same time, we do have voters lists in the hands of political parties, and parties have voluntary measures in terms of privacy.

I noticed that you said there should be a subsidy for political parties on cybersecurity. Is there more that political parties need to do in order to ensure that these voters lists or any other information isn't getting into the wrong hands, even inadvertently?

Mr. Stéphane Perrault: I think that's a very good point. When we issue the lists, we provide with the lists some guidelines, which you have probably seen. If you look at the guidelines, you can see that part of them relate to the legal obligations under the act—the purposes for which this data may be used and so forth—but a number of recommendations are just best practices that we have no authority to enforce.

They are about how you keep track of who in your campaign has those lists, making sure that you recover the lists after the campaign, and safeguarding them when they're not being used by your volunteers. There are important things that campaigns can do and should be doing over and above any legal requirement.

Ms. Anita Vandenbeld: Who owns the data? Who owns that voters list?

Mr. Stéphane Perrault: I don't know that there's a proprietary right. There are certainly legal obligations to use it only for certain purposes under the Elections Act. That's all I can say.

You also mentioned the subsidy. I don't necessarily recommend the subsidy. I think it's something that needs to be examined. I honestly don't know whether parties have the kinds of resources that the evolving threats to cybersecurity require. It's an open question, and I think it's worth considering.

The Chair: Thank you.

Next up for seven minutes is Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair.

Thanks to both of you, Mr. Hutton and Mr. Perrault, for your opening statements. In the interests of time, though, I would like to focus on Mr. Perrault.

Several meetings ago, the investigative journalist and researcher Vivian Krause testified before committee and addressed particularly the millions of American charitable dollars with a stated political objective in the last Canadian election. Those charitable American dollars were sent to Canadian charitable groups, which then transformed the money into legitimate Canadian dollars. They were then distributed in many cases to third parties to be used, presumably, to help further those political objectives of the original American donors.

I wonder if you could address your inability to contain, track and penalize such obvious unacceptable interference with the Canadian electoral process.

Mr. Stéphane Perrault: I won't speak to the specifics of that case. I understand that your question was not about that. As we all know, money is hard to track and limit. Things can be done. The current rules under the act have a number of weaknesses. A number of recommendations have been made in the past, and they're part of Bill C-76.

Bill C-76 goes beyond that. Two main weaknesses are being addressed. The first is that in the past, contributions were made six months prior to the writ period. Because of the way the law is drafted, they were treated as belonging to the entity, so it's their own resources, even though they may come from abroad. The second weakness is that the current law regulates election advertising, which is a narrow category of expenditures. We've seen an expansion of the activities in recent years.

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

The rules are there. They may be difficult to track and enforce, and we'll be working with the commissioner and inviting people who see these things to report these matters to the commissioner so that investigations can take place.

● (1155)

Hon. Peter Kent: Another area of constant concern involves the ability of charitable groups to spend 20% of their revenues, their funds, on political activities. As Ms. Krause testified, the problem isn't political activity. The problem is political activity that doesn't serve a charitable purpose. She recommended removing that completely and saying that charities can spend as much as they want on political activity to support their charitable purpose. However, should it get into partisan politics and support of partisan positions and campaigns in politics, the allowable percentage should be zero.

Could you comment on that?

Mr. Stéphane Perrault: I don't know that I can go very far on that because that's an area beyond my area of responsibility.

Hon. Peter Kent: I think you'd like to be able to.

Some hon. members: Oh, oh!

Mr. Stéphane Perrault: I'll take a pass, if you allow. It may be difficult from a practical point of view. I think whatever the percentage is, it sometimes makes it easier to draw lines for what is partisan, what is political and what is not. I think if you offer some buffer, it may be useful from a practical point of view. I'll keep it at that.

Hon. Peter Kent: Ms. Krause also testified that after a six-month investigation on her part, she filed a report with Elections Canada. Elections Canada representatives went to Vancouver to discuss the contents of that report, which suggested that of 42 charitable organizations investigated by the CRA, 41 were found to be less than compliant, and recommendations were pending that five of them be disqualified entirely as charitable agencies.

Her testimony was that Elections Canada effectively communicated that the agency's hands are tied because the CRA would shut down those investigations, or never report on those audits, and does not share that sort of information with Elections Canada.

Mr. Stéphane Perrault: I want to make a distinction here between the Chief Electoral Officer and the Commissioner of Canada Elections. As members may know, we operate completely independently, and the commissioner is not allowed to share any information with me or the general public on his ongoing investigations unless there's a need to do so. There are exceptions. I'm not privy to the nature or extent of the investigations, the conclusions, or the challenges he would have faced in those investigations.

Hon. Peter Kent: Is the lack of communication between the CRA and Elections Canada a problem in hypothetical terms?

Mr. Stéphane Perrault: Again, I defer to the commissioner on that. I do know that the law in Québec is much more flexible in the sharing of tax information with the *directeur général des élections du Québec*, and that's something that may warrant some consideration in the future. Absent a good understanding of the challenges the commissioner is facing, it's hard for me to go beyond that.

Hon. Peter Kent: You spoke of perhaps considering subsidies or financial support to political parties in their ability to address the new technological challenges. Does Elections Canada have the resources to enforce what you can do at the moment?

Mr. Stéphane Perrault: Absolutely. We are fortunate that the legal structure for the funding of Elections Canada provides a statutory authority to draw from the consolidated revenue, so I can spend what I feel is required and justified to upgrade my IT systems, and I have done that to a significant extent in the last few years.

That is not something that parties have, of course. I can tell you that I understand the costs that are involved there and the challenges that this can represent. I also know that we have a very rich and sensitive database, and it is very similar to that of the parties in terms of its scope on the number of electors. How do they protect that, and how can they take measures?

I don't want to frighten Canadians or members of the committee. I know parties are working with the security partners, and I think that's good news. I just think that, seeing the cost rising for cybersecurity, there is a public interest in considering whether parties have the necessary resources.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for seven minutes is Mr. Davies.

Mr. Don Davies (Vancouver Kingsway, NDP): Thank you, Mr. Chair.

Thank you to the witnesses for being here today.

Mr. Perrault, I'll start with you. Can you say today, as Canada's Chief Electoral Officer, that you are confident that the 2019 federal election is secure against misinformation and disinformation campaigns?

● (1200)

Mr. Stéphane Perrault: We don't control misinformation and disinformation. I am confident that we are taking the steps that we need to take to address misinformation or disinformation about the voting process. I'm confident that we have resources in place—the commissioner has resources in place—to deal with offences under the Canada Elections Act.

But the broader issue of misinformation and disinformation and how information is used to create division within society goes well beyond the roles and responsibilities of electoral management bodies. It's a societal challenge that we're all facing.

Mr. Don Davies: What would be your major concern? If you had one overarching concern about the integrity or fairness or legitimacy of the election in 2019, what would that be?

Mr. Stéphane Perrault: I am quite optimistic about the integrity of the next election. We can't be overly confident, and we have to be alert, but we are taking measures to deal with the challenges.

What is concerning to me when I look at other societies, when there's such a big divide—a polarization—is the lack of an ability to even have a conversation about what is a fair election and what is the legitimacy of an election. I don't think we've reached that point in Canada. I think that's a critical bedrock, to be able to have a consensus on what is fair and what is not fair, and we are doing well, I think.

Mr. Don Davies: I want to direct you to something specific, then. As you testified today and have testified in the past, you pointed out that this committee had recommended that political parties be subject to privacy laws. You yourself have recommended that. I want to quote your remarks. You said:

> If there is one area where the bill failed, it is privacy. The parties are not subjected to any kind of privacy regime. I have pointed this out in the past and I want to mention it again today. The Privacy Commissioner has talked about it, and we are in agreement on this issue. I simply wanted to reiterate that this morning, without going into detail.

Well, I want to take you into a bit of detail, if I can, Mr. Perrault. What are the implications of that failure by the government to subject political parties to privacy laws in terms of the 2019 election?

Mr. Stéphane Perrault: I think what we're seeing is that Canadians increasingly want to understand the nature and the source of the communications that are reaching them. I think an important aspect of understanding that is transparency in the ads and in social media, but another aspect is understanding what data is out there about them and who is using that data, and having some measure of control over that.

While the bill does some good things in terms of the transparency, I do find it unfortunate that it does not go into the privacy side to the extent that it should, which is having minimal standards and some oversight.

Mr. Don Davies: I guess I'm asking why. What's the problem with that?

Mr. Stéphane Perrault: I don't have the answer to that question. It is late in the electoral cycle. I think this is a conversation that we should have had earlier. I realize that the election is now coming, but I don't know any good reason not to have that conversation. I recognize, as I did in answering another member's question, that parties have special situations, and the rules on privacy should be made to apply in a way that recognizes those special situations, but there's nothing that prevents these privacy principles from being used in an adapted manner.

Mr. Don Davies: I want to shift to something different.

Last election, in 2015, I was in Vancouver knocking on doors at 6:15 p.m. pulling the vote—the polls closed at 7 p.m.—when I looked at the TV and saw Peter Mansbridge on CBC call a national Liberal majority. We had many anecdotal reports from people who were counting ballots later in Vancouver that when they turned the ballots over, they could actually determine that the ballots that were cast last took a different hue from the ones that were cast earlier.

Obviously when a portion of the country knows the results of the election before they cast their ballots, not only is that a piece of information that other Canadians do not have when they cast their ballots, but it actually is a piece of information that can influence voting behaviour. Do you have any concerns or proposals to address that in the next election, or do we suffer the same result next time?

Mr. Stéphane Perrault: I don't have a proposal. I recognize the issue. It's an issue that the act has been struggling with over the years. Historically, there used to be a prohibition on the early disclosure of the results in those electoral districts where the polls were still open. The genie is out of the bottle on that in terms of the ability to contain the information because with social media and the Internet, that's very difficult to do.

There remains a staggering of the voting hours. Now, of course, you don't want the people out west to be voting so early that it's not accessible to them. You also have to look at the end of the polling day. If we delay the count or hold the results, we have poll workers —sometimes people who are not young—working for long hours, 16 hours. To extend that period out east so that the results are not disclosed out west would be very difficult on the poll workers. There's no easy answer to that one.

● (1205)

Mr. Don Davies: Thank you.

Mr. Hutton, social media companies are appearing to act more and more like broadcasters of information and news content. In your view, should social media companies be subject to the Broadcasting Act in Canada with respect to those activities?

Mr. Scott Hutton: As you are all aware, currently there is a planned review of the Broadcasting Act and the Telecommunications Act, the acts upon which we undertake our mandate. We've also been asked by government to formulate a report that would feed into those reviews precisely, and that's the report that I referenced in my opening remarks. In that report, one of the main objectives is, essentially, to conclude that any parties who do benefit from operating broadcasting in Canada should be participating in our system.

Hence, our answer would be that, yes, those who are conducting broadcasting should be part of the system.

Mr. Don Davies: Thank you.

The Chair: Thank you.

Next up for seven minutes is Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): I want to thank all of you for being here this morning.

I have a question for Mr. Perrault. We're living in a time when elections have changed. Interference is not only a Canadian issue; it's a global issue. We've seen reports of election interference, obviously, in the United States, France, the U.K. and Germany. We're not an isolated country where only we are facing these types of problems. Our allies, our global partners, are also facing this.

Since our election is coming up next year, subsequent to other countries having had elections in the past, have you had an opportunity to work with your counterparts in other countries to come up with some best practices? I would think that there would be a lot of commonality in approach and tactics. Have you been able to discuss with them what measures they've taken, where they've fallen short, where we can plug the gap and where we can strengthen our own system?

Mr. Stéphane Perrault: Yes, certainly, we have, and we take part in conversations and forums internationally. We've been to Europe and have discussed with European countries their measures. One thing that is striking to me is that the quality of our electoral process and its integrity are no longer just a matter for Elections Canada. We are very independent, and we care about that independence deeply, but we need to work with security partners. We did in the past, but the level of collaboration needs to increase, and it has increased significantly.

We also need to work with parties. I've asked parties to come together, and I'll be meeting with them in the coming weeks to look at what we can do collaboratively. What happens if a party receives a tantalizing offer about hacked information from an adversary party? Are they going to jump on that offer, or are they going to agree not to share it? Whom are they going to call, and how are we going to deal with these scenarios? This is the Macron scenario in France.

We have to look at scenarios with security partners, and we're doing that right now. We have to look at who is doing what and make sure that nothing falls between the cracks. We have to work with parties about what they can do because we all have a shared interest in the integrity of the electoral process.

Mr. Raj Saini: When you talk about the integrity of the electoral process, you're talking about Canadians' access to accurate information in terms of the voting process: where to vote, how to vote and how to register to vote. I want to know what approach Elections Canada will take in an election campaign. Hypothetically, if you see a message on social media someplace about something inaccurate, how do you respond to that? Do you have enough resources to monitor all the social media that are available?

Mr. Stéphane Perrault: We are currently purchasing listening tools. The purpose there is not to listen to particular conversations, and we're not interested in who says what. These are tools that assist with artificial intelligence, gathering information about what's being said about the electoral process. We have key words that we can use. We also have a team that will be working on that, so we will have a strategy with regard to social media so that we can respond quickly if there is disinformation being put out there.

● (1210)

Mr. Raj Saini: I'd like to share my time with MP Erskine-Smith.

The Chair: All right. You have four minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Mr. Hutton, under the Broadcasting Act, broadcasters are subject to some level of quality control of content. Is that right?

Mr. Scott Hutton: According to broadcasting policy, the Broadcasting Act requires that all broadcasting in Canada be of high standard. We take our guidance from that part of the policy. With respect to content, we essentially work in a co-regulatory regime. We enforce a variety of codes that have been developed through public processes with Canadians and with broadcasters to essentially maintain that high standard.

We address issues with respect to portrayal, with respect to news, and so on and so forth. There are also other provisions in our regulations with respect to ensuring that broadcasting of matters that contravene the law, that are abusive, or that are false or misleading news is also addressed through that means.

Mr. Nathaniel Erskine-Smith: What's the smallest broadcaster you regulate?

Mr. Scott Hutton: We regulate through various means. Sometimes we license. Sometimes we do it through exemptions. Some of our smallest broadcasters would be through exemptions. They would be, for example, community broadcasters or indigenous broadcasters in rural and remote areas. You'd probably have companies that have maybe $20,000 to $30,000 in revenue, and maybe a few hundred to a few thousand listeners or viewers.

Mr. Nathaniel Erskine-Smith: So a broadcaster that can reach a few hundred or a few thousand people is subject to that regulatory oversight, yet if I have one million followers on my Facebook page, I'm subject to no oversight at all. Isn't that crazy?

Mr. Scott Hutton: Well, one of the recommendations we've made with respect to the review of the Broadcasting Act and the Telecommunications Act is essentially to recognize that all parties that benefit from operating in Canada live up to the social responsibilities.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Mr. Perrault, you mentioned political parties but not third party political activities.

I have just one example. Ontario Proud has 400,000 followers on Facebook. They say they knocked out Kathleen Wynne in the last election and they're fundraising to knock out Trudeau in the next election. They're not subject to any privacy rules whatsoever. Is that of concern?

Mr. Stéphane Perrault: I want to make sure that this is clear. The Privacy Commissioner will be coming, and you may ask him the question. Third parties in Canada are subject to privacy rules if they are—

Mr. Nathaniel Erskine-Smith: They're not subject to PIPEDA. It's a non-commercial actor, so they're not subject to PIPEDA.

Mr. Stéphane Perrault: They're non-commercial. Yes, that's the nuance.

That's not an uninteresting question, but the Elections Act does not regulate what everybody does at all times. I'm just concerned about expanding here the scope of the Elections Act.

Mr. Nathaniel Erskine-Smith: That's fair, but as someone concerned with public policy, I have greater trust in the Conservative Party of Canada or the Liberal Party of Canada than fly-by-night third parties that can close down operations tomorrow, start up under a different name, and have all that same data to use. Wouldn't you agree?

Mr. Stéphane Perrault: It's quite possible, yes.

Mr. Nathaniel Erskine-Smith: You talked about minimum standards in regulating political activities. I'll just throw out some minimum standards, and you can answer with yes or no.

Would you support real-time ad disclosure, including engagement metrics, the number of ad dollars spent, and the source of those ad dollars?

Bill C-76 goes part of the way, but this would go a little bit further.

Mr. Stéphane Perrault: It would go further, and I would welcome that, yes.

Mr. Nathaniel Erskine-Smith: What about the ability of citizens to request access to personal, identifiable information that third party political actors or political parties hold about them?

Mr. Stéphane Perrault: Certainly, for regulated entities that participate in the election, that's something worth considering.

Mr. Nathaniel Erskine-Smith: Okay. What about penalties for selling information or sharing information improperly?

Mr. Stéphane Perrault: Certainly, penalties for sharing the information obtained from Elections Canada exist in the Canada Elections Act as we speak.

Mr. Nathaniel Erskine-Smith: Last, you mentioned the short time period between now and the next election. Bill C-76 requires political parties to have privacy policies. Should the Office of the Privacy Commissioner have oversight of those privacy policies?

Mr. Stéphane Perrault: My view is that he is the right person to have that oversight, and there should be oversight.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thanks, everybody. We're out of time.

I just have one question for both witnesses. I've been doing a lot of media responses, just about Facebook, Cambridge Analytica and our joint investigation. We're actually going to go over to London and try to hear from Facebook, especially Mr. Zuckerberg.

My biggest concern is the timely response to pull down, let's say, a third party ad that's going to negatively impact a campaign. We all know that the last week in the campaign is crucial, and it can be affected by the littlest of ads.

In terms of a timely response to groups like Facebook and other social media platforms, what do you suggest we do with that to have a quick response that really mutes that immediately?

● (1215)

Mr. Stéphane Perrault: My suggestion is to do as we've done with the commissioner, which is to establish a communication network with them ahead of the election, so that we can alert them to problems during the campaign. That is the most effective way to deal with that.

The Chair: Thank you.

Go ahead, Mr. Hutton.

Mr. Scott Hutton: In our case, we don't regulate the fast pace of the social media platforms. We deal with broadcasters on that front. On our front, all I would add is that one tool we would need is administrative monetary penalties in the Broadcasting Act, to be able to enforce various matters quickly. They are not available to us at this point in time.

The Chair: Okay. Thank you, everybody. Thanks for appearing at committee today. I apologize for the brevity of the presentations. There are a lot of questions to be asked still, but thank you.

We'll wait for the next witnesses to come up. We'll give them about five minutes.

● (1215)

(Pause)

● (1215)

The Chair: I call the meeting back to order.

Again, this is the Standing Committee on Access to Information, Privacy and Ethics, meeting 124, pursuant to Standing Order 108(3)(h)(vii), the study of the breach of personal information involving Cambridge Analytica and Facebook.

This is the second round. We'd like to welcome back Commissioner Therrien, the Privacy Commissioner of Canada; Brent Homan, deputy commissioner, compliance sector; Gregory Smolynec, deputy commissioner, policy and promotion sector; and Julia Barss, general counsel and director of legal services, legal services directorate.

Welcome back, Mr. Therrien. Go ahead for 10 minutes.

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair and members of the committee. Thank you for the invitation to appear before you today.

Last week, I attended the 40th international conference of data protection and privacy commissioners, in Brussels. The conference confirmed what I had explained in my last annual report: There is a crisis in the collection and processing of personal information online. Even tech giants, attending the conference in person or through video, are recognizing that the status quo cannot continue.

Apple CEO Tim Cook spoke of “a data industrial complex” and warned that “[o]ur own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency”. He added, “This is surveillance.” Facebook's Mark Zuckerberg admitted that his company committed a serious breach of trust in the Cambridge Analytica matter. Both companies expressed support for a new U.S. law that would be similar to Europe's General Data Protection Regulation or GDPR.

When the tech giants have become outspoken supporters of serious regulation, then you know that the ground has shifted and we have reached a crisis point.

Your committee clearly senses this ground shift and has supported our recommendations for legislative change. The government, however, has been slow to act, thereby putting at continued risk the trust that Canadians have in the digital economy, in our democratic processes and in other fundamental values.

● (1220)

[*Translation*]

Let's examine, for a moment, the impact of online platforms on privacy and the integrity of elections.

As Canadian artificial intelligence researcher Yoshua Bengio recently said in *Le Monde*: Our data fuels systems that learn how to make us press buttons to buy products or choose a candidate. Organizations that master these systems can influence people against their own interest, with grave consequences for democracy and humanity....The only way to restore balance is to ensure that individuals are not left alone when interacting with businesses. What is the role of governments if not to protect individuals. Nothing prevents regulating against excess and the concentration of power in certain sectors.

In my opinion, these are not uniquely Canadian threats, but global ones.

Aside from the misuse of personal information to influence elections, we have also seen hostile states interfering in elections by deliberately targeting personal data.

ln the words of Giovanni Buttarelli, the EU Data Protection Supervisor:

Never before has democracy been so clearly dependent on the lawful and fair processing of personal data.

Recent investigations in various countries have demonstrated that political parties are harvesting significant amounts of personal information on voters and adopting new and intrusive targeting techniques.

ln July, the UK Information Commissioner released her interim report on Facebook/Cambridge Analytica which found very serious shortcomings in the way digital players are operating.

For example, despite significant privacy information and controls on Facebook, they found users were not told about political uses of their personal information.

The UK Commissioner also raised concerns about the availability and transparency of the controls offered to users over what ads and messages they receive.

Significantly, the UK office found that political parties are at the centre of these data collection and micro-targeting activities. These activities would not take place without political parties.

None of this is encouraging for voters; when we last polled Canadians on this issue, 92% wanted political parties to be subject to privacy law. That's as close to unanimity that one can get in such polling.

ln September, privacy commissioners from across Canada put forward a resolution calling on governments to ensure that political parties are subject to privacy law.

Academic experts, civil society and the Canadian public all agreed with this position; and so does the Chief Electoral Officer.

The government, on the other hand, maintains that while the application of privacy laws to political parties is an issue that deserves study, the next federal elections can take place without them.

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

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

[*English*]

This brings me to updating you on our investigative action. I will be quick here, because I'm conscious of time.

As you are aware, we are proceeding—with our colleagues in British Columbia—with an investigation of Facebook and AggregateIQ. The work is advancing well, but we have not yet made our determinations. We continue to gather and analyze information.

For obvious reasons, I'm limited in what I can report due to confidentiality obligations under PIPEDA. I will remind you that we are investigating, among other things, the access to personal information provided to third parties by Facebook, in particular sharing friends' information with app developers. This was an issue we raised with Facebook in 2009. Since May, we've had many extensive requests for information. We received submissions from Facebook, and we will engage in another round of discussions very shortly.

Our investigation of AIQ focuses on whether it collected or used personal information without consent, or for purposes other than those identified or evident to individuals. Since my last appearance, OPC investigators have issued additional requests for information. They've conducted a site visit. They've undertaken sworn interviews with both Mr. Massingham and Mr. Silvester, and they have reviewed hundreds of internal records from AIQ, including AIQ electronic devices.

In order to make our conclusions public as soon as possible, our plan is to proceed in two phases: one at the end of this calendar year —next month—and a second phase in the spring.

The time for industry and political party self-regulation is over. The government can delay no longer. Absent comprehensive reform, Parliament should ensure the application of meaningful privacy laws to political parties. It should also give my office the same inspection and enforcement powers that most of Canada's trading partners enjoy.

Individual privacy is not a right we simply trade off for innovation, efficiency or commercial gain. No one has freely consented to having their personal information weaponized against them, to use Tim Cook's term. Similarly, we cannot allow Canadian democracy to be disrupted, nor can we permit our institutions to be undermined in a race to digitize everything and everyone simply because technology makes this possible.

Here, we go to the heart of the issue. Technology must serve humankind—that is, all individuals. Without individuality and privacy, it is a philosophical and practical truism that we cannot have a public democratic life, nor can we enjoy other fundamental rights we cherish, including equality, autonomy and freedom. Privacy is the prior condition for the enjoyment of other rights, including democratic rights. Without privacy, the social environment we have in Canada—democracy, political harmony and national independence— is also at real risk, including risks posed by hostile states.

As to the specifics of the legislative amendments that, in my view, might be required, while there are several excellent elements in the GDPR of the European Union, we should seek to develop an approach that reflects the Canadian context and values, including our close trading relationships within North America, with Europe, and with the Asia-Pacific region. A new Canadian law should reserve an important place for meaningful consent. It should also consider other ways to protect privacy where consent may not work, for instance in the development of artificial intelligence. The GDPR concept of legitimate interest may be considered in that regard.

Our law should probably continue to be principles-based and technologically neutral. It should also be rights-based, and drafted not as an industry code of conduct, but as a statute that confers rights while allowing for responsible innovation. It should empower a public authority—it could be my office or another public authority—to issue binding guidance on how to apply general principles in specific circumstances, so that the general principles do not remain pious wishes but receive practical application.

A new law should also allow different regulators to share information.

● (1230)

The Chair: Thank you, Mr. Therrien, for your testimony.

We'll go first to Mr. Baylis for seven minutes.

[*Translation*]

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you, Mr. Therrien.

[*English*]

It's a pleasure to see you back.

Let's go right into the issue of political parties.

We had some arguments made to us that the PIPEDA laws have penalties that are so strict that they would put a chill on political parties' ability to get volunteers, because the volunteers would be subject to these laws and might be fined for inadvertently doing something they shouldn't have.

Is this a concern for you? Have you seen evidence of this? The B. C. laws, for example, have very strict fines. Have you seen this anywhere else, where political parties have been subject to privacy laws? Has there been a so-called chill factor?

Mr. Daniel Therrien: That comment surprises me because, as this committee well knows, I've talked at length about the absence of enforcement powers of the OPC.

Yes, there are some penalties for certain conduct, and as of today, with the new breach regulations coming into force, if political parties were subject to PIPEDA they would be subject to penalties for not disclosing breaches that have occurred.

As a general rule though, as you know, PIPEDA suffers from lack of enforcement, so I was surprised to hear that comment.

Mr. Frank Baylis: As it stands right now, then, that comment does not hold water, in your view.

You were asking for stronger enforcement laws. Let's say that happens and the government gives you the inspection and enforcement powers you seek. Would that chill factor be a concern for you, as the person enforcing those laws?

Mr. Daniel Therrien: Possibly.

First, when I recommend that PIPEDA be applied to federal political parties, it is implicit that context would matter. PIPEDA has a number of principles, such as the right to access information and the right to be clear on the purposes for which information would be used by an entity subject to PIPEDA. The fact that we would be dealing with political parties that have legitimate interests, if not rights, to engage in political discussion with electors would be part of the context.

As we would eventually look at the application of PIPEDA to political parties, certainly there could be an examination of enforcement mechanisms, the amount of penalties and what would make sense for the various entities that are subject to it.

I would end with this. In British Columbia, which is the only jurisdiction in Canada where political parties are subject to privacy law, I believe that the enforcement mechanisms are the same for parties as for other entities subject to that law.

Mr. Frank Baylis: Has there been any chill on volunteers there, that you know of?

Mr. Daniel Therrien: Not that I know of.

Mr. Frank Baylis: Let's compare that to other jurisdictions outside of Canada.

For example, does the GDPR apply to political parties?

Mr. Daniel Therrien: Yes, the GDPR applies to political parties in the EU.

What is the penalty for a political party breaching the GDPR? I must confess I have not looked at that question specifically. We could get back to you.

Mr. Frank Baylis: The argument we're hearing is that political parties are different, that we don't understand and it's a very different world. Political parties say they need to do data differently.

As far as you've seen, you don't agree with that argument. In British Columbia they don't do it. In Europe they don't do it either. Is there any jurisdiction in the world that has privacy laws and has taken an approach where they've said, okay, we have general privacy laws, but we're going to do a whole new set of them, specific ones just for political parties?

Mr. Daniel Therrien: Not to my knowledge, but again I want to emphasize that I recognize that there is a difference in context with the relationship between political parties and electors versus commercial entities and clients. There is a difference in context, but that does not mean that the privacy laws, including PIPEDA, cannot apply having regard to context, as is occurring in Europe or in British Columbia.

● (1235)

Mr. Frank Baylis: That would be within the confines of one law, not two.

Mr. Daniel Therrien: Yes.

Mr. Frank Baylis: I have one more quick question, and then I'll pass it over to my colleague.

Have you looked at the terms of use for all these so-called free applications? I'm talking about free services that I have no choice but to subscribe to. If I want to buy a phone, I have to agree to let them spy on me. I use that word deliberately: spy on me.

If I want to use a company's search engine, so many of the terms of use, which I cannot negotiate, implicitly force me to allow the company to do things I don't want them to do. Then they come in front of us and say, “Don't worry about it. You can just click this button and we won't do it,” but that's not true. What they show you changes, but they do it, and they collect information.

Is any jurisdiction finally coming in with laws that override any company's right to put certain terms of use into the contracts that we have to sign, so we have an overriding one that controls our privacy?

Mr. Daniel Therrien: The short answer is no. What exists in other jurisdictions is rules that have stricter requirements on the conditions for consent, explicit or not, meaningful or not, but not laws that override terms of use of the company. In Europe, for instance, if there are stronger standards requiring explicit consent in many cases, then the consumer, the individual, is better informed of the uses that will be made, but they do not go as far as you're suggesting. Of course, we're looking at this issue on the facts from Facebook in our investigation.

Mr. Frank Baylis: Okay, but I have rights. Say I don't consent. Then they say, okay, you bought your phone, but it can't work. I say that I don't consent to Facebook. Then it says I can't use it. Then I'm blocked out. So I'm looking and I'm saying, as a consumer, as a user, that I want to use these services, but I don't want them spying on me. I don't want them following my data, and I don't want them saying, “Well, you can go and...”, as we had with Google or all these other ones that “tweaked” the wording so carefully.

They have been changing their terms of use all along to give themselves greater leeway to take our data and to use it. I, as a consumer, have zero bargaining power with them, so I must rely on the government.

The Chair: We're at time, so could we have just a quick answer, please?

Mr. Daniel Therrien: I'll just say there are certain things that are truly required for the service to function. For instance, your location must be given to a phone operator so they can reach you. Of course, the issue, from a privacy perspective, is the conditions that are suggested or imposed by companies beyond what is truly required, and there are a lot of them.

Mr. Frank Baylis: If they track me for one year, they don't need that. They need to know where I am today to use it.

Thank you, Chair.

The Chair: Thank you, Mr. Baylis.

We'll go next to Mr. Kent for seven minutes.

Hon. Peter Kent: Thank you, Chair.

Thank you, Commissioner, for appearing before us again today.

Earlier this year, we learned in our study of the scandal with Cambridge Analytica, Facebook and AggregateIQ—as you did in your investigation, and as did the Privacy Commissioner of B.C. and the Privacy Commissioner of the United Kingdom—that millions of pieces of personal data, including that of hundreds of thousands, perhaps more, Canadians, was improperly harvested from Facebook, handled by a number of bodies, and moved back and forth in the digital world across national borders, and we have no assurance that this original improperly harvested data, this mass of data, has been destroyed.

We learned just in the last few weeks that your former Ontario counterpart, Ann Cavoukian, resigned from a Google sibling in Toronto, Sidewalk Labs, because Google could not assure her that highly personal data within Toronto could be effectively de-identified, which Google said was their objective.

Just in the last few days, a Conservative Order Paper question was responded to by the Liberal government regarding recent hacks of the Canadian government: 800 pages, representing perhaps 10,000 hacks or improper access to various government departments and agencies' websites.

This week we learned that you have launched an investigation into Stats Canada's demand or request to Canadian financial institutions for deeply personal information on at least 500,000 Canadians without their knowledge or consent—again, I know that consent is a major concern of yours—to develop a new institutional personal information bank. The claim here by Statistics Canada is that it would be anonymized.

Certainly, after seeing Cambridge Analytica, Facebook and AggregateIQ, and after hearing the very legitimate concerns of a well-recognized authority like Ann Cavoukian over the impossibility or the unlikelihood of de-identification being achieved, I'm also deeply skeptical about Statistics Canada's ability to guarantee that all of the information they're harvesting will be anonymized.

I know you've just begun your investigation, but is consent a paramount consideration in situations like this? Could we have your comments, please?

● (1240)

Mr. Daniel Therrien: You've described a number of situations. Consent is certainly a fundamental principle of PIPEDA, in the relationship between consumers and commercial organizations. However, as I said in my opening remarks, I think it would be useful to consider whether consent, given the complexity of technology and business models, will always offer a meaningful privacy protection, or whether we should look at other mechanisms, such as legitimate interest under the GDPR. That's for the commercial sector.

With respect to the public sector, consent is not as fundamental. It is an element, but there are a number of situations where the government can require, from an individual's data, personal information for service delivery. If I put the two together, the use of information either to deliver government services or to offer services for a company, I think it's important to recognize that data can be useful to either the public or the private sector to offer better services.

The issue is how to properly manage that information and—very importantly, from my perspective—have the right legal framework to ensure that the actors, whether it's government departments or companies, handle that data in a responsible way. It should also ensure that there is a third party, currently my office, with powers to protect individuals, because individuals will not be able to protect themselves completely when facing large corporations or large departments.

I'm not against the collection, use and sharing of information to improve services, but I think that our current frameworks in Canada are lacking.

Hon. Peter Kent: Would you consider that this sort of request should at least take into account the consent aspect? In other words, a great many Canadians, as we've seen across the country, have reacted to this breaking story with outrage that their most personal financial secrets, if you will, attached to their SIN numbers, would be collected without their consent.

Mr. Daniel Therrien: Statistics Canada is arguing that they can do this without consent based on the current legal framework. Because we're besieged with complaints, my obligation is to consider these arguments, consider what complainants will say and come up with a conclusion.

Hon. Peter Kent: We don't know what system they are using to collect the data, to hold the data, and to anonymize the data, whether it's just by attaching a code number, but if they're going to use it in the way that has been described, it would seem that as long as they have that data, it is accessible to a potential breach. A breach of this sort, of deeply personal financial information, could have political overtones in terms of the way it might be used if that information was not successfully held.

● (1245)

Mr. Daniel Therrien: I put it in terms of the legal principles at stake. Financial information is sensitive; therefore, it is deserving of a higher level of security safeguards. We have not looked at the security safeguards put in place by Statistics Canada, but as a matter of principle, the nature of the information in question would require a high level of security safeguards.

Hon. Peter Kent: Do we have any idea which technology company would be employed by Statistics Canada?

Mr. Daniel Therrien: We'll find out when we investigate.

Hon. Peter Kent: We don't know whether Google might be the data collecting or data—

Mr. Daniel Therrien: I doubt it, but we will find out soon.

The Chair: Thank you, Mr. Kent.

Hon. Peter Kent: Thank you.

The Chair: Next up for seven minutes is Mr. Davies.

Mr. Don Davies: Thank you, Mr. Chair.

Commissioner, you have provided an exceptionally clear and profound description of the fundamental role of privacy in a democracy. You've used terms like “crisis point”. You've said that the lack of protection puts the public trust at risk; that citizens' personal information has been weaponized; that this leaves our elections open to manipulation and it jeopardizes the fairness of elections. You have said that parties are at the centre of data collection. Of course, you've also mentioned that 92% of Canadians want political parties subject to privacy laws as the prime actors using that information, yet this government has refused to apply privacy laws to political parties.

Have you heard of any persuasive reason offered by government for why privacy laws would not be properly applied to political parties, in terms of protecting the privacy of the information they have?

Mr. Daniel Therrien: Going back to the context issue that we discussed a few minutes ago, I've heard the argument that political parties need to be able to have some freedom to communicate with electors as part of the democratic process leading to a party being elected.

If we look south, for instance, in the United States, these kinds of arguments actually have a constitutional foundation at the level of principle. But as a matter of practice, is the communication between parties and electors impaired because privacy laws apply to political parties? From a practical, concrete perspective, we know of a number of jurisdictions where political parties are subject to privacy laws, and in these jurisdictions no one is saying that subjecting parties to privacy laws has, in effect, impaired the quality of the discussion between parties and electors.

Theoretically, perhaps, there is an argument that can be made, but on the ground, it has not been borne out where these laws apply, and I have not seen evidence—although I hear the argument and it's an interesting argument—that the quality of the communication would be impaired if political parties were subject to privacy laws.

Mr. Don Davies: Mr. Baylis touched on this. Of course, British Columbia, the province that I come from, does in fact subject political parties to privacy laws. Are you aware of any diminution in the democratic ability of parties to participate?

Mr. Daniel Therrien: No.

Mr. Don Davies: You have pointed out context, I think, quite properly—that there are differences in context between commercial and political purposes—but I'd like to focus on the similarities.

Businesses are selling a product. Political parties are selling a candidate, a platform. Businesses are selling a widget and are seeking money to purchase their widgets. Political parties are seeking donations. They're both advertising.

Appreciating the context, is there any principled reason that privacy laws that do apply to private actors should not apply to political parties?

● (1250)

Mr. Daniel Therrien: I'll repeat that there is this argument made about the quality of communication, but I, at least, have not seen evidence of an impairment in the quality of the communication between parties and electors.

Mr. Don Davies: I want to read from a political party's website, I won't tell you which one. It says this: “It is also possible that your information could be provided to us by a volunteer or friend who thinks you would be interested in getting involved with [the party].” Would that respect any privacy law or consent regulations currently in force in the country with respect to the consent principle?

Mr. Daniel Therrien: Let's look at this example. It's an interesting example. If you apply privacy law, strictly speaking, consent has not been obtained. Therefore, the party in question should not receive the information. But in order to have a communication between a party and an elector, I think I'd be interested in looking at that situation, the first communication. A friend says to party A, my friend B may be interested in hearing from you. So the party has information about friend B. One of two things happens: Either friend B says, “Yes, I'm interested”, and then the communication continues; or friend B says, “I'm not interested”, in which case I think a proper application of privacy laws would have the information being set aside and the communication stops.

The first part of the sequence may be an example where context may lead to a different application in terms of the outcome, even though the privacy principles would apply.

Mr. Don Davies: It asks whether you'd be interested in getting involved with the party; it's not asking to be contacted. Does that change your concern at all?

Mr. Daniel Therrien: No, I think what I've said would apply.

Mr. Don Davies: We heard a reference to the information that Sidewalk Labs' controversial waterfront smart city project has created some concerns. We've heard that Ann Cavoukian, the Ontario privacy commissioner, resigned from her advisory role over her concerns about privacy protection.

Has your office been looking at that project, Commissioner? Are there any privacy concerns on your end that you're investigating?

Mr. Daniel Therrien: We have been in touch with Sidewalk Labs under a new advisory program that we created a few months ago as a way to bring companies to comply with PIPEDA, in this case. We want to work with the willing and have discussions on how best the company may bring about an operation in a way that is PIPEDA-compliant. We have had a number of conversations, which at this point are still at a very high level of generality. We are engaged in this process. We've not gotten down to the level of concrete details where I could say whether I am concerned or not. It's at a very conceptual stage at this point.

The Chair: Thank you, Mr. Davies.

Last up, for seven minutes of shared time, we Mr. Picard and Ms. Fortier.

[*Translation*]

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Thank you, Mr. Chair

Thank you very much for being here once again, Mr. Therrien.

We've met several times during our study, and I think it's important for you to be here again today to give us a progress report.

With regard to your investigation and update, you said it's difficult for you to communicate information. Do you have an idea of the date when you can issue your report?

Mr. Daniel Therrien: We'll try to do it in two stages. Under the act, we have a year to complete our report. We'll obviously try to do it sooner. One year takes us into the spring.

Mr. Brent Homan (Deputy Commissioner, Compliance Sector, Office of the Privacy Commissioner of Canada): Yes.

The first phase will be in December, the second perhaps in the spring.

Mr. Daniel Therrien: That's it.

To disclose our findings as soon as possible, we want to present our report in two stages so that some are made public in December and the latest ones in the spring.

Mrs. Mona Fortier: At this point, do you think you've assembled all the necessary information? The committee has tried to raise certain questions. Do you have the necessary resources and information to complete your investigation?

● (1255)

Mr. Daniel Therrien: We've had several discussions with the two companies in question. To date, we've received the information we requested. We're now in the process of validating it.

Do you want to add anything, Mr. Homan?

Mr. Brent Homan: We're gathering information from the two organizations, Facebook and AggregateiQ, and verifying other information with the groups.

Mrs. Mona Fortier: It's very clear from your recommendation that you want the privacy laws to apply to Canadian political parties. Thank you for telling us that.

I'd like to know whether you think we should have a review or perhaps new measures respecting third parties. We've discussed that issue at length.

Do you have anything new to say on the subject? Do you think we should have other provisions respecting third parties?

Mr. Daniel Therrien: In British Columbia, the equivalent act to PIPEDA applies to all entities, including non-profit organizations, because all organizations engaged in commercial or other activities compile information that includes some information of a delicate nature. Those organizations should be subject to the same provisions.

With regard to third-party organizations—I was in the room when you discussed that kind of organization in Ontario—I think the act should apply to all organizations engaged in commercial or other activities that compile, use or transmit personal information.

Mrs. Mona Fortier: Thank you.

I'm going to turn the floor over to my colleague Mr. Picard.

Mr. Michel Picard (Montarville, Lib.): Thank you.

Good afternoon, Mr. Therrien.

We understand that you're seeking better oversight, better control and greater powers. I'm frankly not opposed to the idea. I think we need to keep an eye on what's going on. However, I don't get the impression we're seeing what needs to be changed or controlled. It's fine to want better control and the resources you need in taking more radical action to address a problem, but first you have to define that problem. I'm not sure we've properly done that. I think we've been spreading ourselves a bit too thin for some time now. I'm going to outline a scenario for you, and then I'd like you to comment on it.

Companies request information from a client. The client provides it, starting with his name. The number of details that are then requested vary from one company to the next. As my colleague said, if, as a client, I fail to provide a minimum amount of information, I won't have access to services. I also can't do much about criminal behaviour from the outside. If I'm hacked, that's not necessarily attributable to bad faith or inappropriate policies. You can always fall victim to some internal or external deficiency, and there are some things I can't control. However, when I register for a service, I expect to receive most of what the supplier is willing to provide me. So that's a relationship between two parties.

I don't think the problem is to determine what information I provide. We're told that, for reasons of transparency, we need to know what businesses do with that information. However, if they start telling us what they do, that is to say, exactly what they were previously doing without our knowledge, that won't change their professional practices much. We won't be any further ahead even if they're very transparent.

The issue isn't to determine what's going on. The problem we have to address, and which may goad us into finding better ways of proceeding, is that we lose all control of the situation when a third party enters a transaction.

Rather than try to control everything that happens, wouldn't it be preferable to establish in actual fact that the information provided to a service provider—and that includes a person's name—is private and must not be communicated, regardless of what type of information it is? So, if I do business with a third party and it wants to use my information to send me ads, so be it, but my personal information would never be disclosed to others, even if I provided it.

Should we focus on transactions involving a third party? In your efforts, you could cooperate with the Competition Bureau, for example.

● (1300)

Mr. Daniel Therrien: In the guidelines that we've proposed and that will come into force on January 1st, we state in particular that companies should be more transparent with consumers. However, that includes their exchanges with third parties. If I understand correctly, you'd like to go further and propose a measure that's tantamount to a prohibition from disclosing information to third parties. Is that correct?

Mr. Michel Picard: The idea isn't to prevent the service. It's possible to advertise without disclosing information.

Mr. Daniel Therrien: Absolutely, but various kinds of transactions involve third parties. Imagine a company that provides a very specific service and contracts its accounting or other secondary functions to a third party. Should we prevent the principal company from dealing with a third party in such cases? Not necessarily.

I think a partial solution is to be very clear about third parties and to give consumers a genuine option to prevent disclosure where third-party intervention is not needed to provide a service. Prohibiting a company from doing business with a third party would obviously protect privacy, but do we need to go that far? I don't think it's necessary.

Mr. Michel Picard: Thank you.

[*English*]

The Chair: Thank you, Mr. Picard.

Thank you, everybody.

Again, thank you, Commissioner Therrien, for having an abridged presentation. I know it's tough to squeeze it all into 45 minutes or less. I appreciate your efforts on the file, too. I know there's a lot to cover, and I know you're spread on multiple fronts, as we are. Thanks for you presentation today.

Mr. Daniel Therrien: Good luck on the rest of your study.

The Chair: Thank you.

The meeting is adjourned.