HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 102 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, April 26, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 26, 2018

● (0845)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): We'll call to order this morning's meeting of the Standing Committee on Access to Information, Privacy and Ethics, meeting number 102. Pursuant to Standing Order 108(3)(h)(vii), we're doing a study on the breach of personal information involving Cambridge Analytica and Facebook.

This morning, as individuals, we have Colin J. Bennett, professor in the department of political science at the University of Victoria, and Thierry Giasson, professor in the department of political science at Université Laval. In our second hour, we have Marshall Erwin with the Mozilla Corporation.

We'll start off this morning with Mr. Bennett.

Prof. Colin Bennett (Professor, Department of Political Science, University of Victoria, As an Individual): Thank you, Mr. Chair.

Can you hear me okay?

The Chair: Yes, we can hear you very well.

Prof. Colin Bennett: Good morning. I'm delighted to be with you again today and to appear with my colleague, Professor Giasson.

I am a professor of political science at the University of Victoria. I have been studying and publishing on privacy protection issues for around 30 years in Canada and internationally. In 2012, I co-wrote a report for the Office of the Privacy Commissioner on the use of personal data by Canadian political parties. Since then, I have been researching the nature and influence of data-driven elections in Canada and overseas, and I have been warning about the implications for privacy and other democratic values.

The current controversy that you are investigating raises a range of interrelated issues, and it is important to carefully distinguish them. There is the monopoly power of companies like Facebook in the platform economy, the harvesting of data on one's social network through third party applications, violations of campaign spending limitations, issues concerning the accountability of targeted political ads, cyber-threats to election integrity, the larger role of big data in our elections, and what I really want to talk about today, which is the role political parties play in data-driven elections and their relationship with our regime of privacy protection.

Cambridge Analytica and AggregateIQ are part of a larger voter analytics industry. There are many other companies, mainly American, that have taken advantage of more flexible privacy standards in the U.S. and the ability to process vast amounts of personal information from public and commercial sources, used to micro-target consumers in an increasingly granular manner.

There has been a lot of hype about the importance of big data in elections and recent scholarly work that sheds a skeptical light on the extent to which data analytics do indeed influence election outcomes. Nevertheless, the competitiveness of current elections continues to place enormous pressure on major political parties in most democracies to continue to use data analytics to gain any edge over their rivals. Thus, more data on voters are being captured, and those data are increasingly shared through a complicated and dynamic network of organizations involving some quite obscure companies that play important roles as intermediaries between the voters and their elected representatives.

This industry is not as extensive in Canada, but there is still a large variety of businesses that offer various services on polling, data analytics, software development, digital ad placement, social media outreach, and so on. We lack a comprehensive understanding of the role that personal data plays in the political process in Canada, and we lack an accurate picture of this industry. I'm going to let my colleague, Professor Giasson, speak more about this.

I have followed your hearings very carefully. The investigation is an important beginning, but it is only a beginning, and we need a lot more analysis. I would like to make three general points about policy development going forward.

My first point is the critical importance of bringing Canadian privacy law in line with the GDPR. The recent decision of Facebook to move the data on all its non-European users from Ireland to the United States is motivated in part by a desire to escape some of the more stringent rules inherent in the GDPR. To discourage this kind of jurisdiction shopping, it is critically important that Canada raise its privacy standards to make it more difficult for companies to engage in this kind of behaviour. Your February report is an excellent start.

Particularly critical for these issues about the processing of information on political opinions, which is defined as sensitive to data in the GDPR, is the need, first, to strengthen PIPEDA's consent provisions; second, to implement provisions for algorithmic transparency, as you advise; third, to make privacy by design and default central legislative principles in PIPEDA; fourth, to strengthen the Privacy Commissioner's audit and enforcement powers; and last, to clarify those categories of sensitive personal data, including those on political opinions.

My second point is that there is a pressing need to bring our political parties within Canada's regime of privacy protection law. I have testified about this to you before. One of the keys to preventing the kinds of abuses we've seen in other countries is to establish some clearer and consistent rules on the kinds of data that political parties may use for campaigning purposes. We need to establish a level playing field that essentially prevents companies like Cambridge Analytica from engaging in the same practices in Canada that have been witnessed elsewhere.

● (0850)

We are one of the only advanced democratic countries where privacy protection law does not cover political parties. For the most part, they are not covered by PIPEDA. They are not government agencies. They are not covered by the Privacy Act. They are also largely and expressly exempt from the anti-spam legislation, as well as from some of the do-not-call list regulations administered through the CRTC. There are privacy and security rules within the Canada Elections Act, but these apply to the voters lists, not to other sources of personal information.

Thus, with respect to political parties, Canadians do not have the legal rights that they have with respect to both government agencies and commercial operations.

Moreover, whereas the Privacy Commissioner can investigate Facebook, he cannot investigate the practices of our political parties, so he cannot get the full picture in the way that the Information Commissioner in the U.K. can, and is, under her current investigation.

There are four legislative options with respect to regulating federal political parties: the Privacy Act, the Canada Elections Act, PIPEDA, and stand-alone legislation. There is a need for serious legal and constitutional analysis about the various legislative options, because each approach has its pros and cons. I could go into this in the Q and A, if you'd like.

However, it does appear to me that the status quo in this respect is untenable. First, there is going to be continuing publicity about the use of personal data in elections, which will only increase leading up to the federal election of 2019, particularly with respect to political micro-targeting on Facebook.

Second, it should be noted that political parties do have to comply with B.C.'s privacy law, the preferred Personal Information Protection Act. The commissioner in B.C. is currently investigating the practices of B.C.'s provincial parties. I believe, as do many, that federal political parties are also governed by this legislation to the extent that they are capturing information on voters in B.C. If federal parties have to comply with B.C.'s privacy legislation, which is consistent with PIPEDA, then there is no sensible reason why they should not extend those same good practices across the country.

Third, I do sense a growing recognition among parties that pursuing good privacy management practices is in their interests, as well as those of citizens.

Finally, therefore, my third point is that political parties should self-regulate as far as they can to improve their privacy policies and practices. Legislative change might take some time. In the meantime, though, there is much that parties can do to self-regulate and restore public confidence.

I have analyzed the privacy policies of federal and provincial political parties, and the commitments that have already been made. I've shared this paper with the committee, and I understand it's being translated.

There have been some improvements since our 2012 report, but they are still incomplete and, in my view, inadequate. None provide clear commitments against all 10 principles contained in the national privacy standard, which is at the heart of PIPEDA.

I don't see why all parties can't publicly endorse these principles and adhere to a common privacy code that comprehensively addresses the protections for all personal information under their control. It's not enough, but it would create a more level playing field. In 2013, the Chief Electoral Officer recommended that adherence to such a code be a condition for receiving the voters list. It's unlikely that one party would pursue such a course on its own, so leadership will be necessary, involving the CEO and the Privacy Commissioner.

In my view, in terms of what should change, there should be greater transparency on the sources of data, captured directly or indirectly, that enter parties' voter relationship management systems; a common commitment that parties do not and will not purchase commercial sources of personally identifiable information; an agreement on how social media platforms should, and should not, be used for electoral purposes, particularly with respect to automated bots; commitments to privacy accountability, including designated chief privacy officers, and better training of staff and volunteers on privacy and security; stronger commitments to provide rights of access and correction to individuals; better management and updating of internal do-not-call lists; a common commitment to provide unsubscribe options for email and text messages; better management of the access to party databases; and clearer policies about how to respond to data breaches.

None of this should be difficult or contentious, and I don't think it should be a party-political issue. Political parties have a responsibility to educate and mobilize the electorate, but there should also be an appropriate balance between their important interests and roles and the privacy rights of Canadians.

● (0855)

No organization likes data breaches—just ask Facebook. Just think of the ramifications of a major data breach for any political party in the course of an election campaign.

Thank you very much for your attention.

The Chair: Thank you, Mr. Bennett.

Next up is Mr. Giasson, for 10 minutes, please.

[*Translation*]

Prof. Thierry Giasson (Full Professor, Department of Political Science, Université Laval, As an Individual): Thank you, Mr. Chair and members of the committee.

My name is Thierry Giasson. I am a full professor in the department of political science at Laval University. I am also the director of the Groupe de recherche en communication politique.

To start, I would like to thank you for your invitation to share with you the findings of some of my work on how political parties collect and use data from digital tools and media. I would like to recognize the importance of the study you began a few weeks ago further to the media reports about Cambridge Analytica and possible ramifications for Canadian citizens.

To avoid going over the same information that my colleague Colin Bennett will be sharing with you, I will limit my remarks to how political parties in Canada and Quebec currently collect and analyze digital data.

Many of you are of course familiar with these practices. However, as your proceedings are public, and the average Canadian citizen is less familiar with these practices, I thought it was worth explaining them for the benefit of the general public.

My presentation focuses on three areas.

First, I will talk about some of the current practices for collecting personal information that political parties use for electoral marketing purposes or political communications. I will then examine what types of personal data political parties use, and how they compile it.

Second, I will introduce the objectives associated with analyzing this data and the analysis methods preferred by the parties. I will examine why political parties analyze data on Canadian voters.

Last, I will go over some of the implications for Canadian democracy associated with using Canadians' personal digital data.

To begin, what data is compiled by political parties, and how is it collected?

First of all, it is important to mention that collecting and analyzing Canadians' personal data has been part of the political marketing process that political parties have used for more than 30 years, but it has increased dramatically in the last 15 years or so.

Political marketing involves an in-depth analysis of segments of the population so that election decisions can be made that will help the party identify the electoral districts and segments of the electorate to focus on during the election campaign in order to generate votes. The entire process is intended to help the party gain votes.

The purpose of political marketing is to create more targeted voter messaging and, ultimately, to win elections. The more accurate and extensive the data, the higher the quality of the analysis will be. For many years, election marketing was based on survey data and discussion groups. In the past 10 years, however, parties have also been using personal data collected online, primarily because that data is geotagged.

When a person has an account on a social media platform, they often provide their postal code, for instance, which pinpoints their location very accurately. This gives political parties a very precise, almost granular level of detail on voters. All these forms of data are added to analysis platforms and run through various mathematical procedures or algorithms. We will come back to this in a moment.

The political parties collect personal information in three main ways. First, several months before an election is called, Elections Canada and the other provincial election bodies give the parties access to all the personal information on the voter registration list. These lists provide citizens' names and addresses and so forth. To this initial data, the parties then add aggregate data from national surveys carried out for the parties by market research firms, and from research reports produced by organizations such as Statistics Canada. In addition, for the last decade, parties have been mining citizens' personal information online. This data may be volunteered or it may be provided to political parties without the citizen's knowledge.

Political parties collect information when voters provide their email address, postal code or phone number on the party website, when they attend a partisan event, or when they sign an online petition sponsored by the party on a specific issue.

This information is given willingly to the political parties by citizens. However, most people don't know what the parties do with it. Moreover, as my colleague Colin Bennett pointed out, the parties are not required to tell them what exactly they will do with that information.

● (0900)

Next, parties can collect information on voters by studying users' social media usage. All the major social media companies such as Facebook, Google, and Twitter offer their corporate clients various forms of aggregate data on how people react to the messages that political parties post on social media platforms. These companies also offer consulting services to political parties to develop targeted communication campaigns for specific sub-groups of users.

Lastly, and this is rarer in Canada, political parties can also purchase personal digital information on Canadians through companies specializing in that field. Those companies sell data on the consumption habits or debt levels of customers, for example. These data brokers are commercial intermediaries that generate databases using various methods, more or less legally, and sell the information, almost always without users knowing it.

For example, that is what AggretateIQ, the Cambridge Analytica intermediary, was doing. It harvested personal information on users through a digital application linked to Facebook, which Cambridge Analytica then resold to its clients to be used to target voters and certain segments of the population.

Why do parties collect data in this way, and how is the data analyzed?

As parliamentarians and active members of your respective political parties, you are well aware that Canadian political parties are seeing a drop in membership and funding, while at the same time voters are more flexible in their party loyalties and more critical of our political institutions.

Many of the strategists I interviewed as part of my research told me that the leaders of Canadian political parties now have to overcome major organizational hurdles to win an election. In the last 20 years, they have turned to political marketing and digital communication to try to generate new human and financial resources.

As political marketing integrates into contemporary campaign development in Canada, it does so in a context of major technological change. Election preparations and political marketing combine traditional approaches to political organization and emerging approaches that, as you know, involve a variety of online and offline platforms.

Influenced by the technological innovation used in the American presidential elections in 2008, 2012, and 2016, political parties now make digital tools a central part of their election preparation process. This has led to the emergence of a new category of political strategists specializing in social media, computer scientists, mathematicians, and software engineers, a whole cohort of data analysis specialists. These people did not work for political parties 15 years ago, or were responsible for creating websites or disseminating content at that time. They were not necessarily responsible for focusing specifically on election campaigns. These digital strategists are now at the centre of organizational processes and election campaigns.

In 2004, the Conservative Party of Canada was the first party to use a voter analysis system linked to a database with personal information on Canadian voters. Leading up to the 2015 election, the NDP and the Liberal Party also developed their own databases to target voters, and collected and analyzed citizens' information. Segment profiling is done using computer-based algorithms that identify the co-occurrence of socio-demographic and political characteristics among voters, whose information is aggregated in databases.

The parties now collect this information on voters in a permanent database, particularly through online advertisements and social media applications such as Twitter and Facebook. Political parties pay these companies to access the metadata of their subscribers. Geotagged information from social media provides the parties with information on users' socio-demographic characteristics, how often they visit that social media platform, and what they like or share.

Using political marketing leads the parties to develop election platforms that are more targeted and tailored to individuals. The party's position addresses the priorities of a select group of voters, their targets, who are identified during the market study and selected based on their potential for a positive reaction. For example, this targeted approach led the federal Conservatives to make niche commitments, such as the tax credit for tools for people in the trades, the universal child care benefit, and eliminating the federal long-gun registry.

Once again, digital technology is used for communicating these hypertargeted messages. Targeting election communications ensures that party messaging reaches the micro-audience that it is exclusively intended for.

● (0905)

Everything done online, including collecting and analyzing Canadians' personal digital information, has the end goal of putting the parties in direct contact with individual voters and persuading them to get out and vote. You can appreciate that the obsession with winning the election will always be the driving force behind what political parties do, and that includes collecting and using personal information.

In conclusion, this brings us to the risks to Canadian democracy that these practices may pose. While they do help political parties overcome the strategic challenges I mentioned earlier, in my opinion and in that of various other Canadian researchers, these emerging election organization practices compromise the quality of our democracy and our civic duty. The growing use of political marketing and voter analytics is largely taking place behind closed doors, unbeknownst to Canadians. This restricts both the representation of interests and information sharing, thereby progressively eliminating the concepts of the common good and public debate.

Exercising citizenship and election choices...

[*English*]

The Chair: Mr. Giasson, we are one minute over. Are you just about done?

Prof. Thierry Giasson: I'm just about done.

The Chair: You have 30 more seconds, and then we'd better move to questions. Thank you.

[*Translation*]

Prof. Thierry Giasson: That's perfect.

Despite growing media interest in the role of voter analytics and algorithms in election campaigns, everything that is going on, including the Cambridge Analytica affair, is being done without Canadians' knowledge, and most Canadians are largely unaware of the extent and effect of the parties' use of their private data. This has a major impact on our democracy.

So I call upon you, members of the committee who are examining these issues, to try to provide serious food for thought for the government to consider in order to establish a better framework for the use of this information and to ensure that Canadians fully understand how their information is being used.

Thank you.

● (0910)

[*English*]

The Chair: Thank you.

First up, we have Mr. Erskine-Smith, for seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks to you both.

I want to start with transparency in advertising. My question is for Mr. Bennett, or for you both, actually. When it comes to the targeted nature of ads, we've always had targeted ads in politics in different ways. People advertise in specific magazines because they think that this readership is more likely to respond to a message, as indicated in your opening comments. If there is a particular issue that Canadians might be interested in because they have kids or because they own a gun, or whatever the case might be, messages get targeted, and really always have been. It's often information that is not collected digitally, but collected at the door. A real issue seems to be the transparency in the targeted nature of these ads.

I don't know if you're aware, but Mr. Wylie was just before Congress and proposed some recommendations for transparency in political advertising. Perhaps you could both speak to the importance of transparency and what that transparency actually looks like in practice.

Prof. Colin Bennett: Perhaps I'll defer to Thierry first on that.

[*Translation*]

Prof. Thierry Giasson: Thank you for your question.

I think that is the crux of the matter and what is of interest to the entire population, I would say. There is no transparency right now. Can you hear me?

[*English*]

Do you hear me?

Mr. Nathaniel Erskine-Smith: I don't have translation.

Prof. Thierry Giasson: I'll say it in English. That's fine.

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

The Chair: Sorry, Mr. Giasson. You can go back to French. Your English is very good, but our translation should be working now.

[*Translation*]

Prof. Thierry Giasson: As I was saying, transparency is the crux of the matter. There has in fact always been targeted communication.

[*English*]

Are you not hearing anything?

Mr. Nathaniel Erskine-Smith: It's not working for me. I'm not sure why.

With respect to transparency, I'll propose two solutions. One solution is that, when political parties put out ads online, there be a central repository that's accessible to the public to see all ads that have been posted. Individual campaigns can submit them in a public fashion to Elections Canada, which would then have them posted in a central repository. There are different solutions to this, but all ads must be made publicly available to individuals who are concerned about the targeted nature of these ads.

Second, if I receive a targeted ad on Facebook or otherwise, I should be able to see the underlying characteristics that made up that targeting: whether it's because I'm between the ages of 30 and 40, or I am a white male, or I have an interest in baseball or whatever the case might be. I should be able to see the specific characteristics that the campaign has selected to reach me.

Do you think those two solutions are sufficient, and if not, what else should there be?

Prof. Colin Bennett: I'll speak to that. My understanding is that Facebook has started that process in an experimental manner in Canada to identify the sources of ads that are targeted in Canada. Yes, I agree with that. It's also worth noting that those kinds of procedures would pretty much have to be in compliance with GDPR if this is done, and it is done in Europe. That's an important note.

I'll just add one other thing concerning the social implications of the lack of transparency. That creates, of course, an incentive for candidates to say one thing to one group of voters and another thing to another group of voters, because it is not transparent. That has also been shown to contribute to the phenomenon called the filter bubble, in which there is no common discourse across a political system about solutions to public problems.

● (0915)

Mr. Nathaniel Erskine-Smith: This is my last question, and then I'm going to pass it over to my colleague Ms. Fortier. Which one of you is most expert in PIPEDA?

Prof. Colin Bennett: That would probably be me.

Mr. Nathaniel Erskine-Smith: We had representatives from Facebook before us, and they indicated that 272 Canadians gave consent to an application that shared the personal information of over 600,000 Canadians, including possibly private messages.

In your view, given your understanding of PIPEDA, is that in compliance with the existing law?

Prof. Colin Bennett: No, I don't think it is. Furthermore, Facebook has been under investigation by the Office of the Privacy Commissioner since 2009. This whole issue about access to people's personal information through third party applications was investigated back then. Audits were ordered back then, and still the problem persists. I personally don't believe it is in compliance. It is non-consensual capture of data on Canadians, and my own view is that it would be in contravention of PIPEDA, although we would have to see what the Privacy Commissioner says. It would certainly be in contravention of the GDPR.

[*Translation*]

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

I have a quick question.

In the by-election that I won last year, in Ottawa—Vanier, a situation arose between a third party and one of my opponents who wanted to bring forward a certain issue.

Do you think this kind of conduct could pose a risk in an election campaign? Do you think third parties will make greater use of online platforms during their campaigns or is it hard to track that kind of coordination?

Prof. Thierry Giasson: That is an excellent question.

The electoral communication of third parties is of course governed by the Canada Elections Act. The courts have in fact issued numerous decisions that forced Elections Canada, around the year 2000, to review part of its legislation in this regard.

I think the digital dimension complicates the work of the heads of elections monitoring agencies such as Elections Canada, Elections Ontario, and Elections Quebec. I think they would be the first to admit that they do not necessarily have the human resources needed to do this work. I think we need to review the resources allocated to these election assessment agencies and give them all the resources they need to do this important media monitoring work. Having a diversity of platforms for political communication is all well and good, but for elections regulation officials that means having the resources to investigate all these platforms. So there is a multiplication of platforms which, in my opinion, makes the monitoring work of elections officials more complex.

[*English*]

The Chair: Thank you.

Next up is Mr. Kent, for seven minutes.

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

Thank you, both, for attending by video conference today.

Since my late-life involvement in partisan politics in 2006, every election has seen new technologies available for use and new ways of accumulating, analyzing, and applying data to identify the voters who are supporters and those who are not. A lot of what we are hearing in this particular study of the vulnerability of our democratic electoral process with regard to the inappropriate use of user data by Cambridge Analytica or Facebook is where to draw the line.

In my experience, it is as Professor Giasson outlined—identifying voters through the electoral list, through responses or clicks on social media or political party sites, or through volunteers coming forward and providing their information.

Where would you suggest we draw the line on accumulating a certain number of data points on Canadian voters? We are told that, in the case of Facebook and Cambridge Analytica, they accumulated in their so-called information warehouse as many as 5,000 data points on more than 230 million Americans, obviously to be applied in a way to compromise or interfere with the democratic process through the vulnerabilities or preferences of those social media users. Where would you suggest we draw the line in Canada?

● (0920)

[*Translation*]

Prof. Thierry Giasson: I invite you to get with the times and recognize that holding elections in 2018, 2019 or 2020 is not the same as it was in 1998. I think you have summarized that very well, sir.

There are things that political parties could decide to stop doing or that we could no longer allow political parties to do. Personally, I think the use of social media should not be allowed. I think that for all the information that is gathered when people visit your organizations' websites or through your online petitions, there should be a box explaining what you will eventually do with the information. That way, citizens would clearly understand that when they give you their telephone number, their email address, and their postal code, this information will be entered into a database and used in targeting to determine whether or not they are interesting voters for your campaign.

Citizens do not have access to that and you do not tell them, which leads some media and researchers like myself to say that political parties are in a sense spying on citizens, collecting information without their knowledge, and using that information to manipulate public opinion during the election campaign.

I think a modern elections act should provide a very strict framework for the use of data from social media. You already have enough information at your disposal to do the kind of targeting you need to do without necessarily also collecting this information and storing it in your databases.

[*English*]

Hon. Peter Kent: Thank you, Professor. I certainly agree, and I think my colleagues around this committee table would agree, that transparency in terms of the acceptable use of voter data would certainly address the concerns of people who have suspicions that it might be misused. I think that, in 2015, *L'actualité* basically accused all Canadian political parties of spying on Canadians.

In your remarks, you talked about data brokers, not the accumulators of data, but the brokers who come in to figure out ways to apply that data to effect a certain electoral outcome. You said that these intermediaries who generate databases use various methods more or less legally. Are you aware of any cases of illegal use of political party databases in Canada?

Prof. Colin Bennett: One of the problems with the lack of transparency is that you don't really know where the illegality might be. There are certainly a lot of grey areas here.

In response to your question, however, I would make just two quick points.

It's very important for the committee to note that Cambridge Analytica is one of several companies that do this. Claiming to have 5,000 data points on citizens is actually not uncommon. There are several companies I could point to in the United States that do similar things. The thing that brought Cambridge Analytica to public and media attention was its use of psychographics, which I think most Canadians would really feel crossed the line. However, again, I'm not sure that it would actually be illegal.

In my judgment, the 10 PIPEDA principles provide the guidance here. In the paper I submitted to the committee, I've gone through all 10 principles and explained how our political organizations can, and should, comply with all of them. The parties already do, to some extent, but it's not complete. My plea is not only for transparency here, but also for uniformity, whereby there would be a common agreement among our major federal political parties on what is acceptable practice, online and off-line, with respect to all the sources of personal information captured on Canadians.

● (0925)

The Chair: You have 10 seconds.

Hon. Peter Kent: I'll hold my question for the next round.

Professor Giasson, did you have a comment?

Prof. Thierry Giasson: Yes. Based on the research and the interviews I've done with strategists from federal parties and Quebec-based parties, the purchasing of data from third parties or information brokers is very rare. The only instance that was documented, by a few colleagues of mine, was of the Conservatives buying some data from third parties on consumer habits. We don't know if this data was collected illegally, but I would presume not.

From the testimonies I got in my research, this is a very exceptional practice. It's not common.

The Chair: Mr. Masse is next up, for seven minutes.

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair.

Thank you, gentlemen, for appearing today.

Perhaps I could follow up on the 10 standard principles. Unfortunately, we don't have the paper in front of us. Did you include in that submission a grading of the different political parties? Would it be fair to say that the larger political parties have an advantage, or at least a more probable case of being able to meet those standards for financial reasons, such as having internal supports and money used to ensure that those standards are actually met?

Specific to that, how does another party get started in Canada if the encumbrance is too much with regard to that? How do we not stymie democracy with that?

Prof. Colin Bennett: That's a good question. I don't grade the political parties. It's very difficult to do this on a common standard.

The experience in B.C., where political parties have had to comply with our legislation, which is pretty much based on the PIPEDA principles, has been quite encouraging. One of the things it forces parties to do is to consider internally all the different sources of personal information they have.

One of the difficulties with what I see at the federal level is that it is not clear what these privacy policies apply to. Some of them are based on data captured through the website, and some of them are more general.

To your point about smaller political parties, I actually think this is a way to level the playing field and allow smaller political parties into the game more effectively. This is one of the effects of social media as well. It should not be a costly compliance exercise.

Opposed to that argument, of course, is the cost of a data breach. Any organization that has suffered a major data breach will know that the costs of that, in terms of finance and reputation, are far in excess of the costs put in up front to develop a clear privacy code and some transparency for the Canadian electorate.

Mr. Masse, you asked an extremely good question. It needs far more analysis, but that would be my response at the moment.

Mr. Brian Masse: This is my sixth term here, and I've seen blatant electoral fraud, which has even had the consequence of members of the House having to resign from their active seat.

To follow up, would it enhance our democratic response? I know that we have chronic underfunding for the Privacy Commissioner, the Competition Bureau, and the Chief Electoral Officer, but if there were rules prescribed, for example, by an independent body like the Chief Electoral Officer, with an enforcement mechanism, in terms of how data is accumulated and used, and those responsibilities, which would be enforceable by punishment of law, in an ideal world, would that be the way to govern a set of rules that would then be applied across established political parties or those trying to find roots in Canadian democracy?

Prof. Colin Bennett: I think that this would be one approach, yes, but my plea is for some more detailed legal analysis on this. I think one of the dilemmas here is that the Chief Electoral Officer knows political parties and knows the regulations on political parties, but he is not necessarily resourced and adept at dealing with privacy issues. The Privacy Commissioner has those skills and resources but doesn't have the legislative mandate to do that, so it falls between the cracks. The other institution that is responsible here is the CRTC, of course.

I think there will have to be some very careful legislative and constitutional analysis on this question. In the meantime, I don't see any reason why there couldn't be a code of practice agreed to, under the auspices of the Privacy Commissioner and the CEO, perhaps jointly, that would have the effect of establishing a more level playing field, establishing more transparency, and preparing for the day when legislative rules come in.

● (0930)

Mr. Brian Masse: Do you have anything to add there, Professor Giasson?

Prof. Thierry Giasson: I agree with what Dr. Bennett said.

Mr. Brian Masse: What's your opinion with regard to third party use of accumulated data by political parties? One of the things I have a concern about, and I think Canadians do as well, with regard to Facebook and other data accumulation models, is the unknown fact of where data can go and how it can be used. It would require a major policing effort to try to even enforce such laws.

At any rate, how egregious do you think that is for democracy, the fact that political parties can either bring in third parties or use third parties to augment, support, and use the data they have?

Prof. Colin Bennett: To your first point about transfers of data, I think this is where the rules concerning the GDPR are so relevant. Europeans are insisting, of course, that for any data transferred to Canada there be strong onward transfer restrictions. Facebook and other private sector organizations have to comply with those rules. That's point number one.

With respect to the rules about consent and political parties, I think that bringing the entire ecosystem, if you like, into a similar set of rules would allow an organization like the Privacy Commissioner to see the entire picture in the way that the Information Commissioner in the U.K., at the moment Elizabeth Denham, is able to do.

The Chair: You have 30 seconds.

Mr. Brian Masse: You mentioned spying. Spying is more of a proactive approach, as opposed to a recipient approach in terms of data. Can you maybe highlight where you think the political parties might be spying? My interpretation is that it requires more of an overt effort, as opposed to just accumulating data and using it.

Prof. Thierry Giasson: Go ahead, Colin.

Prof. Colin Bennett: These words get thrown around in the media and, of course, they're not necessarily accurate. I think it's the lack of transparency and trust that creates that kind of discourse. I believe that political parties have a fundamental and important role in our democracy, and they need personal data in order to reach out to Canadians, but there needs to be a balance struck. The PIPEDA principles, I think, provide exactly the right set of standards by which that balance can be effectively struck. Moreover, when they were developed back in the 1990s—and I was part of that process—the application of those flexible principles to situations exactly like this one was anticipated. Then they became part of PIPEDA.

That would be my answer to your question, sir.

The Chair: Thank you, Mr. Masse.

Next up is Mr. Saini, for seven minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning to both of you, gentlemen. Thank you very much for appearing.

Mr. Giasson, I want to start with you.

I was very interested in a study you did, which you published in the *Canadian Journal of Communication*. It was done during the 2011 election campaign. You put McGill students through different political ads, both negative and positive, and you measured their response physiologically and cognitively.

I am wondering if you could review the results of the experience, and the specific difference you found between a positive and a negative ad.

[*Translation*]

Prof. Thierry Giasson: Okay.

We conducted an experiment to see if negative election ads evoke different reactions from people, as compared to the ads that we researchers call “promotional advertising” and that you just called “positive advertising”. Instead of attacking its adversaries, the party promotes its platform, record or team. We found that people responded to negative advertising with heightened attention. Their pulse quickened.

We measured people's pulse, as well as cutaneous sweating. We also asked people to spontaneously indicate their first impression after each ad. We refer to that as “spontaneous cognitive responses”. This method is very commonly used in social psychology to measure people's level of cognitive engagement.

We realized that election ads, especially ads that attacked the party that the elector supports, triggered cognitive processes to protect the ego. People tried to find arguments to destroy the negative argument that was presented. Based on the increase in skin conductance and pulse, we realized that people responded more intensely to negative ads.

In short, that is what we concluded from that work. The type of ads people are exposed to triggers different physiological and cognitive reactions.

● (0935)

[*English*]

Mr. Raj Saini: After reading your article, I noted, and you reiterated the same point, that there is an increased attentiveness when you see negative ads. Right now we see a lot of negative ads circulating on the Internet.

There are a couple of pieces that I want you to comment on, to see what sort of reaction these extreme ads would provoke. I was in Latvia, travelling on a different committee, prior to the deployment of Canadian forces there. One of the things we were briefed on was that some disinformation would be occurring and to be aware of it. We've seen examples on the Internet where Canadian soldiers are being accused of doing certain things, which is total disinformation. We also saw that in Nigeria during the election campaign, where some very horrific images were used against one political party.

If negative ads are increasing attentiveness, what kinds of reactions are they going to provoke in the people who watch them?

[*Translation*]

Prof. Thierry Giasson: It focuses our attention, but that often quickly triggers mechanisms to protect our partisan opinion.

When shown an election ad that attacks the party that the person intends to vote for, or that they belong to or campaign for, ego protection mechanisms are activated in people's cognitive processes to deconstruct the argument presented. This focuses our attention and triggers a stronger cognitive process, but there is not necessarily a ripple effect. If the ego protection mechanism works, it will instead lead us to establish our partisan position more firmly and protect us from the potentially persuasive effect of the advertising.

Of course, I have not studied the cases you mentioned so I could not comment on them. In the case in Africa that you mentioned, we could assume that the citizens who support the party being attacked will use an argument, more or less consciously, to protect their political convictions concerning the party under attack.

[*English*]

Mr. Raj Saini: Do I have any time?

The Chair: You have two minutes.

Mr. Raj Saini: The reason I was interested in your paper—and Mr. Bennett can also comment on this—is that we have a realm called the Internet and as technology gets more specific, there is more micro-targeting of certain individuals with the information we have. My concern is whether that micro-targeting can be used in an extremely negative way to influence someone to do the wrong thing, whether it be terrorist activities or other things. How worried should we be that this micro-targeting can influence someone, as you said, in a heightened response, heightened attentiveness? Is there something we can do? What is your advice? Is that a worry for you also?

● (0940)

Prof. Colin Bennett: I think we have to make some distinctions between forms of micro-targeting. Of course, the more innocuous form is where particular segments of the population are singled out for messaging about a particular policy proposal. On the face of it, there is nothing particularly controversial about that. I would just point out that the actual business model of Cambridge Analytica was based on the belief that different individuals, with different psychological characteristics, would respond emotionally in different ways to similar messages about policy, both negative and positive. Most Canadians would find that something we do not want in this country.

One key to it is advertising standards, so that's part of the picture, but of course another key to it is what political parties can and cannot do in using commercial sources of data and these companies in their campaigning. It's a complicated picture involving different sets of legislative standards in Canada, as well as different institutions.

The Chair: Thank you, Mr. Saini.

Last up, we have Mr. Bernier, for five minutes.

[*Translation*]

Hon. Maxime Bernier (Beauce, CPC): Thank you, Mr. Chair.

My question is for you, Mr. Giasson. In your opening statement, you mentioned that democracy has evolved and that political parties now use somewhat more sophisticated data to achieve their ends. Before that, there were polls. Actually, parties still use polls to gauge what's popular and what isn't with a view to being elected and better representing their constituents. That's part of democracy. Wanting to know which policies are supported by the electorate in order to win elections and better represent it can be seen as a positive for democracy.

Normally, polling companies have to state who they are when surveying the population. Respondents know the name of the company conducting the poll and for which political party they're doing it. Today, things are more complex. The Internet and social media are sources of information from which to develop more targeted policies. This can lead to better representation.

The issue you raised relates to lack of transparency. People don't know that, in order to win elections, political parties use information to “better represent them” and bring forward policies that suit their needs.

What are the best practices in the area? The issue of transparency came up earlier. What can we do to ensure greater transparency so that political parties can keep polling their constituents—which, again, is a positive for democracy? What federal legislation or regulation needs amending so that people know what's what whenever they click on an online petition or what have you?

Prof. Thierry Giasson: Your use of quotation marks around the notion of better representing people is significant, as it's really a matter of perspective. Some would say that the data isn't used to represent people, but rather to better target them. After all, we're only really talking about “some” citizens. You're playing semantics a bit, Mr. Bernier. We're not talking about the electorate as a whole.

You know just as well as I do that, when the leader of a political party addresses the Canadian people, they aren't talking to each and every Canadian man and woman, but indeed to a particular segment of the population, about issues that matter to those voters. They aren't really talking to however many Canadians are not in that particular segment. The analyses of polling data and personal information show that those other Canadians are much less likely to react positively to the party in question. So, we're playing semantics a bit, but the quotation marks you used in your remarks are very significant.

Data are in fact being used and transparency is therefore of critical importance. It lies at the heart of the issue we are facing today. The Canada Elections Act needs an overhaul to address, on the one hand, the issue of how political parties can collate data, and on the other, the whole question of research. The act allows political parties to spend money on research during a campaign, but it doesn't clearly define what is meant by research.

If we decide to allow political parties to compile personal information on voters in Canada, the issue needs to be well defined according to specific parameters, in the Canada Elections Act as well as in the Privacy Act.

We will need to make political parties subject to the regulations governing privacy protection and management of personal information. There is legislation on the books that restricts the types of related activities that different kinds of organizations can engage in, but it doesn't apply to political parties. These need to be brought back into the Canadian regulatory framework so that we may restrict what they do with their information and ensure that it complies with the basic principles of the Canada Elections Act. We also need to develop mechanisms that would ensure greater transparency within political parties.

Earlier, in response to a question posed by your colleague Mr. Kent, I gave the example of someone who accesses the Conservative Party of Canada's website. Whenever someone accesses your or any other party's website, a little window pops up to welcome them, asking for their e-mail address, and even their phone number and postal code. The data is then collated, but no one tells us what it will be used for. It would be easy to have a little dialogue box pop up with “Yes, I agree” and “No, I disagree” options that would alert the constituent as to the possible ways in which the political party in question might use their information.

It's still a bit like the wild west right now; we don't know what you're doing. That's why we need to make some key information available to people, but also to ensure that political parties are subject to new elections and privacy regulations.

● (0945)

Hon. Maxime Bernier: I have a quick question for you.

In order to win elections in the future, will political parties have to increasingly target special interest groups, lobby groups, or Canadians who want to gain specific advantages from the government? Is that the future of politics or can a politician have a future by advocating for broader policies without targeting lobby groups?

Prof. Thierry Giasson: One does not preclude the other.

[*English*]

The Chair: Could we have a very brief answer, please?

[*Translation*]

Prof. Thierry Giasson: I can say that all political parties, including yours, already do that.

Hon. Maxime Bernier: Thank you.

[*English*]

The Chair: Thank you.

The last question goes to Mr. Baylis.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Professor Bennett, you put up three policy ideas. The first one, as I understand it, is that our Canadian policy should be in line with the GDPR. The second one is that you'd like to see political parties brought under PIPEDA. What was your third point? Did I understand correctly that you would like to see a voluntary code of ethics? Is that what you're proposing?

Prof. Colin Bennett: I think legislation is necessary, but I also think that it requires some analysis. PIPEDA applies principally to commercial organizations. Political parties are not commercial organizations. There is an argument that at the moment when political parties are purchasing data on consumers commercially, they are indeed subject to PIPEDA to the extent that they are engaging in those transactions, but that might be contentious.

My point is that there are four ways to get here. There are at least four legislative regimes: the Canada Elections Act, the Privacy Act, PIPEDA, and stand-alone legislation. PIPEDA provides the principles, but I'd like to see the Privacy Commissioner do some analysis on this and come out with some recommendations, perhaps jointly with the Chief Electoral Officer. That's going to take some time. In advance of that, I would like to see the political parties declare publicly that they comply with the 10 privacy principles in the national standard. I think the NDP has already said that publicly, but I'm not entirely clear.

The final point I'd make is that when it was revealed that Mr. Wylie had worked with the Liberal Party, there was immediately a debate in the media about that. That led to responses from the different political parties about what they do and do not do. The process has already begun in terms of becoming more transparent, and I would like to see that extended so that every political party takes a good, hard look at what political data it captures on Canadians and how it captures it online and off-line, and do exactly the same kind of good due diligence privacy management that is expected of the commercial sector.

● (0950)

Mr. Frank Baylis: Just a simple thing, then, do you see a pledge to follow the principles as an intermediary step before we get around to proper legislation?

Prof. Colin Bennett: I would like to see a code of practice. This was actually recommended by the Chief Electoral Officer in his report a few years ago. Compliance with that code of practice would be a condition for receiving the voters list.

It's an interim step. I don't think it is enough, because a third party, such as the Privacy Commissioner, would need to have the ability to investigate if there are complaints. However, I don't see why that couldn't be done initially. If I understand what Minister Scott Brison said publicly, the government is looking at that option, and I think it would be an interesting first step.

I would also emphasize what I said about British Columbia. I think there is going to be increasing pressure on political parties in B.C., because of our law, to comply with the legislation here. If that occurs, it only makes sense for political parties to comply with the same standards across the rest of the country. It shouldn't be difficult and it shouldn't be contentious, but I realize that this has been said about other issues.

Mr. Frank Baylis: Thank you.

Ms. Vandenbeld, go ahead.

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

Mr. Giasson, I believe you were talking about the GDPR, and one of the elements was algorithmic transparency. Can you explain how parties are using algorithms and what that transparency would look like?

[*Translation*]

Prof. Thierry Giasson: It was Mr. Bennett who was talking about the general data protection regulations in his presentation. I talked about algorithmic data analysis in my presentation.

As I explained, the parties collect data from various sources. The aggregate data is entered into a data base and then run through algorithmic processes, statistical analysis for social sciences, and logistic regressions. The co-occurence of a certain number of socio-demographic and political characteristics are identified in order to create voter profiles.

We determine the connections between these various voter profiles and those who traditionally vote for the party. The data base provides the parties wtih information on their own voters. That helps them to determine the profiles that line up most with their voters from a socio-political perspective, and then choose the voter who might potentially vote for them if the party puts forward certain policies.

The algorithms are there to process a disparate volume of data and give them meaning in order, in fact, to make it possible to profile voters. Essentially, that is now the focus of the digital strategists, software engineers, or computer scientists who work for political parties.

[*English*]

The Chair: Thank you, Ms. Vandenbeld.

We're definitely at time or a bit past, because we started a little later. I want to say thank you, especially to Mr. Bennett, who is surprisingly fresh being up testifying at 5:45 in the morning. As well, Mr. Giasson, thank you for appearing before the committee.

We're going to suspend for about five minutes until we bring in the next witness. We're also going to grab some time for committee business at the end.

● (0950)

(Pause)

● (0955)

The Chair: I'd like to welcome everybody back to the Standing Committee on Access to Information, Privacy and Ethics.

Now we have before us the Mozilla Corporation, which is being represented by Marshall Erwin, director of trust and security.

Mr. Erwin, go ahead for 10 minutes.

Mr. Marshall Erwin (Director, Trust and Security, Mozilla Corporation): Thank you.

Today is a challenging time for the Internet, particularly as it relates to the collection, use, and sharing of people's personal information from the web. These challenges are demonstrated by the breach of trust involving Facebook and Cambridge Analytica, but they are not unique to those companies.

We as an industry, in partnerships with governments and committees like this one, have a responsibility to build a healthier Internet ecosystem that gives people meaningful control over their privacy. Mozilla appreciates the seriousness with which this committee is taking this issue, and we thank you for inviting us here to express our views.

My name is Marshall Erwin. I am the director of trust and security at the Mozilla Corporation. My role primarily involves working with our product and engineering teams to understand the privacy properties of the Firefox browser to make sure that, within that browser, we are practising the same principles that we preach on a day-to-day basis regarding privacy.

First, I am going to talk about Mozilla's approach to privacy, and then I'll talk a bit more generally about our perspective on where the industry is.

Mozilla is a mission-driven organization dedicated to creating an Internet that truly puts people first, where individuals shape their own experience and are empowered, safe, and independent online. That commitment to our mission is why, when the story regarding Facebook and Cambridge Analytica first broke, we made the decision to pause our advertising on Facebook. That advertising remains paused today.

That commitment to our mission also lives within the Firefox browser that we produce and that is used by hundreds of millions of people around the world. We practise a set of data privacy principles within that browser that shape the data collection we have.

Firefox is essentially your gateway to the Internet. As such, the browser, the piece of software that runs on your computer or your phone, will manage and have access to a lot of sensitive information about you and about the websites you visit. That is information that stays on your device; Mozilla does not collect it. As a browser-maker, we actually don't know very much about how our users browse the web or about their interests. That is a big challenge for us, but it's also by design. If you are using the Firefox browser to do something sensitive or personal, you can have confidence that Mozilla is not going to learn about that.

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

Mozilla has a set of policies and processes in place to govern the data collection we have. I can talk about these in a lot more detail, but what I think is important for this committee to understand is that it is possible to build a product that hundreds of millions of people use that collects some data by default while respecting the users' privacy and not putting that privacy in jeopardy. That is what we have done at Mozilla with the Firefox browser.

It can be difficult to find the right balance between privacy and the features that people want. This is not easy. We believe that we strike the right balance with the browser. Unfortunately, that is not where the rest of the industry is today.

Let's talk a bit about the technology industry, where it is doing well, and where it needs to improve.

The technology industry, especially its biggest players, is doing a decent job providing people with privacy controls. If you are a Facebook user and you care about your privacy, you can take steps to limit what data the company retains and what data it shares with others. However, the industry is coming up short in three areas that I want to call your attention to.

First, those privacy controls are often buried and difficult to find. The industry does not proactively help people understand and use their privacy settings. As a result, Internet users might have technical privacy controls, but they do not have meaningful control over their privacy today.

Second, the default state of those controls is not reasonable and does not align with users' expectations of what will happen when they use a product or a service. Users are defaulted into the collection and sharing of sensitive data. This violates what we call the sensible settings principle that we practise within Firefox. These sensible settings do not exist for much of the technology industry today.

Third, the data collection and sharing that are tied to those privacy settings are still expansive and permissive. The basic limited data principle—again, one that we practise within Mozilla—is not one that is followed by the industry.

If you examine the issues regarding Facebook and Cambridge Analytica, you will find that all those issues are at play.

I want to call the committee's attention to one specific issue that deserves further consideration, which is the collection and use of people's browsing activity as they navigate the web, sometimes referred to as cross-site tracking on the Internet. This type of activity is often associated with the Facebook's Like button.

● (1000)

If that button is on a website that you visit, and irrespective of whether you click that button, Facebook may collect data about the page you visited and use that data in targeted advertising.

The three problems within the industry that I identified are all still present here. Internet users do not have meaningful control over this tracking activity, nor do they even understand that it exists. The default is to track users across the web, and there are few limits on the data collection through that tracking. This tracking is a problem. It creates privacy risks and it undermines the basic trust that people have when they go online today.

Facebook argued before the U.S. Congress two weeks ago that its cross-site tracking activity is no different than what companies like Twitter, Pinterest, and Google do every day. Facebook was right about that. This is a common tactic across the industry and is not unique to Facebook in any way. However, we are at an important inflection point. Organizations like Facebook should be asking what they can do to lead the industry to some place that does not involve tracking people across the web without giving them meaningful control over that tracking.

There is a critical role for committees like this one to play in pushing Facebook and other companies to explain their cross-site tracking activity, to state plainly whether they believe their users understand and have meaningful control over that tracking, and to articulate what they are doing to lead the industry to a better place on this issue.

Again, I want to thank the committee for inviting us here today. I look forward to answering any questions you may have on Mozilla's overall approach to privacy or the perspectives that we have on the industry.

● (1005)

The Chair: Thank you for your testimony.

I just want to say to committee members that, with the time limitations that we have, we have to be crisp. If we go to seven minutes times four, that's 28 minutes.

First, we have Mr. Picard.

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

I'm happy to hear about the way Firefox is working, because I do use Firefox. When I use Firefox, I am just getting at someone else's page. When I end up on Facebook, or Amazon, or whatever page, what is the role of Firefox while I'm looking at these pages? Is it still on and does it still monitor my activity? Since I'm using your browser, does it know, first, that I am on Facebook and, second, what kind of activity I have on Facebook?

Mr. Marshall Erwin: When you are using Firefox and you navigate to Facebook, the browser is still on. It is still running on your computer. What that means is that potentially Firefox can know what you are doing on Facebook and then could potentially provide that information to us. Again, I say "potentially", because that is not what we do. We very purposefully do not do that. We don't feel that this is the appropriate role for the browser. That is why we have a set of policies in place to govern the data collection that we have—exactly what Firefox gets to know about your activity on Facebook, and what data Firefox, the software running on your device, actually tells Mozilla.

As I said, although potentially any browser can monitor your activity and then disclose that activity to the company that makes the browser, that is not the position we are in or want to be in. We do not want to know about your activity on Facebook.

Mr. Michel Picard: If you allow me, I'll switch to French.

[*Translation*]

Currently, "potentially" is a dangerous word in the industry. It opens the door to all manner of technological development.

What type of data, other than that of users in real time, do Firefox or Mozilla obtain from third parties to develop their own marketing?

[*English*]

Mr. Marshall Erwin: It's important to know that there are a few types of data that, again, potentially could be accessed through Firefox. We divide that data into three categories. The first is what we call technical data. For example, this is data about the operating system that you're using when you use Firefox. The second is what we call interaction data, which is data about how you engage with the browser itself. The third category of data that we identify is web activity data, like the URLs that you browse to or the fact that you visit Facebook.

Our data collection focuses on the first two categories by default. A useful example to keep in mind here is the back button. We collect data from Firefox to understand how people are using the browser, so if you hit the back button, it's useful for us to know that this is something you are using to navigate through the tool. We do not collect data about the page you were on when you hit that button, or the page that you are navigating back to. We want to know how you are experiencing the browser, but not information about the websites and how you are interacting with those websites.

● (1010)

[*Translation*]

Mr. Michel Picard: If I understand correctly, the various visits by a user on various sites or pages is the third category of data for which you do not retain information. In other words, the existing technology can follow the activity of one person on the different sites that person visits.

Is that data available? An extreme example related to criminal activity comes to mind. If we need to know whether such and such a person visited such and such a site, that data is available through your technology.

[*English*]

Mr. Marshall Erwin: It's important to distinguish between us and the party that you might be engaging with when you visit a website. If a law enforcement entity came to Mozilla and said that it needed information about someone's web-browsing activity, we largely would not be able to satisfy that request. It is data that we do not have and do not collect. There is the cross-site tracking I mentioned earlier, which happens sometimes by third parties using Firefox. Those third parties might have that data, and a law enforcement entity would have to go to them to get it.

[*Translation*]

Mr. Michel Picard: Why should I provide any personal information to a service for which I am not offered any services or products? Let me explain. If I use the Mozilla browser and use a social network such as Facebook, I am using a service to talk to people, to get information.

I do not have a business return as such. The opposite is true when I register on my bank's virtual site, for example, and I buy books on Amazon, since I need to have merchandise delivered. If I need to make transactions through my bank, then it makes sense that I provide personal information.

Why should I provide information from the outset? If I do not need to provide information for this type of service, then why is the provider making the effort to collect what little information it can to which I never consented?

[*English*]

Mr. Marshall Erwin: You mean, why would Firefox have the means to do that? We don't. Firefox is a piece of software running on your computer. As such, like any piece of software running on your computer, it has the potential to do a lot of things. The question is, what does it do? It doesn't collect that data at all.

[*Translation*]

Mr. Michel Picard: Your business seems to be small relative to the rest of the market.

Are you saying that the service you offer would be the best model for service providers that do not market goods? A social network, unlike an online store, has no good reason to collect personal data. In your case, by all accounts, you can operate without access to that information.

[*English*]

Mr. Marshall Erwin: I think our technology raises a different set of privacy challenges than a social networking service. I would say, though, that the set of principles we stand for on privacy are applicable to both. In practice, it would take some work by a company to translate that into questions of what data it should collect and how its consent model works. Those principles apply both to Mozilla and to those other companies.

Over the last two decades, essentially, in really seeking to make those principles meaningful within the browser, we have successfully built a product that is very respectful of people's privacy. I think that if other companies were to take those principles and translate them into their technology, they would be able to do the same.

The technology itself might raise a different set of issues and questions about what the consent model is, what data is collected, what a company learns, and what it's not going to learn. Those answers will vary based on the technology, but I think the principles still apply. Again, practising those principles has allowed us to build a browser that we feel is quite respectful.

● (1015)

The Chair: Thank you, Mr. Picard.

Next up is Mr. Kent, for seven minutes.

Hon. Peter Kent: Thanks for being here with us today.

Over recent years, but particularly in the last six to eight weeks, there has been an awful lot written and opined with regard to the rush and the focus by social media companies to use new technologies, evolving technologies, and artificial intelligence to add to their business plans and profitability.

The five data privacy principles of Mozilla, and the restraint you described in terms of not going where other social media companies have gone, have obviously affected your profitability. How does Mozilla compare with Facebook in terms of annual revenues?

Mr. Marshall Erwin: Off the top of my head, I would say it's a different piece of technology, much smaller than Facebook in terms of total revenue.

Our revenue model is a bit different. We have partnerships with search providers. When you search within Firefox, you land on a search page, and we get a portion of the revenue generated from those searches. Our revenue is much smaller than that of Facebook.

Hon. Peter Kent: When Mozilla withdrew its advertising from Facebook, what was the primary reason? Was it the unwillingness to be associated with Facebook as the scandal was evolving, or was it fear that your advertising was vulnerable to abuse?

Mr. Marshall Erwin: I would actually give you a slightly different reason. We looked at the settings, the third party data-sharing settings that existed within the Facebook platform when that story broke, and it was clear that, at a minimum, those settings were not sufficient or transparent, and possibly not accurate.

Also, as I mentioned, overall across the industry there is a problem with the default state of settings. I think you could see that in where those settings were that day. The default was still set to sharing fairly expansive data with third party app developers.

When we looked at those settings, we thought that this was just not the right level. It didn't appear to be accurate or transparent, and the level of sharing was still too broad. It was a moment when we could take a stand and say, “We are not going to advertise, at a minimum, until those settings are fixed.”

Hon. Peter Kent: Your biography tells us that you began your career in the intelligence community. You worked for five years as a counterterrorism and cybersecurity analyst, and you have done work for the Congressional Research Service on National Security Agency surveillance leaks and legislative changes.

Given your background and your career, would you consider the Cambridge Analytica/Facebook scandal a matter of national security in the United States or in Canada?

Mr. Marshall Erwin: That's not the way I—

Hon. Peter Kent: I mean with regard to democratic election interference, or attempted interference.

Mr. Marshall Erwin: Overall, if you look at what has happened with the election, you'll see that there are critical challenges to our democratic processes today that are certainly national security challenges. I haven't really thought through the specifics of Facebook and Cambridge Analytica, so I wouldn't be prepared today to say that these specific issues are national security ones.

Overall, the level of data collection that is happening across the Internet, coupled with the new and innovative ways to get messages to people, has raised a host of challenges to our democratic institutions. Certainly those have materialized in terms of national security issues.

Hon. Peter Kent: Facebook has made it clear, although with very unclear answers, that it does not like the GDPR. I think Mr. Chan, the Canadian representative for Facebook, said that Facebook would accept some regulation but made it quite clear that it would not be the GDPR. Would Mozilla accept the GDPR regulations as they are about to come into effect in Europe next week?

Mr. Marshall Erwin: As they come into effect in Europe, we are accepting them.

Your question and the question that I know this committee—

● (1020)

Hon. Peter Kent: Would you accept them in the United States?

Mr. Marshall Erwin: What we want in terms of a regulatory regime is a principles-based approach, one that does not micro-manage the technical decisions that companies are going to make. That's point one that we think is a priority.

The second point is a strong enforcement regime that gives those regulatory requirements their teeth. When we think about this in the United States, in Canada, and in Europe, the question is, does the right set of principles apply? Is that in place, and is the enforcement structure there?

Specifically with respect to Canada, with PIPEDA, I am not a PIPEDA expert, but I think you do have a strong foundation in place. You might consider changes to align PIPEDA with the GDPR, but I think it's important that you actually have a good baseline. A baseline does not really exist in the United States today.

Hon. Peter Kent: Enforcement is the problem.

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

Hon. Peter Kent: I have one minute to go.

With regard to the ownership of browsing data, Mr. Zuckerberg didn't make it absolutely clear, but in his testimony in Washington he said that the content generated by a user is owned by the user. However, he was very fuzzy with regard to browsing history. Is the browsing history on Mozilla absolutely protected, or are there ways that third parties could track it and use it?

Mr. Marshall Erwin: Again, we do not collect that browsing history. It remains on your computer. That means it's protected from Mozilla, essentially. We could always change the browser, but we've made a commitment that we are not going to do that.

I mentioned that the cross-site tracking that occurs across the industry does provide many different parties with access to people's browsing activity. Those third parties can't access your expansive web browsing history in the Firefox browser. If you are on a particular page and then you navigate to another page, and if those cross-site tracking technologies exist on both pages, third parties can collect information about the fact that you visited both of those pages. Over time, that allows those parties to build a fairly expansive data set of people's browsing activity.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up is Mr. Masse, for seven minutes.

Mr. Brian Masse: Your decision to go with the model that you have right now with regard to not collecting that expansive data and not using that from your product is a business decision, for a variety of reasons—for ethics, and for those who would be more concerned about privacy. Is that accurate? Is it less about capability, and more about a business decision to restrict that?

Mr. Marshall Erwin: I would think about it a little differently. What are the incentives we have to do the right thing? Those incentives aren't just limited to business issues. Mozilla Corporation is a public benefit company. We do not have a set of stockholders for whom we need to maximize revenue. That's a critical component of why, in the end, we make the decisions that we make.

We also have a user base that really cares about its privacy, and a set of developers who work with us who also care a lot about its privacy. That factor really influences our decisions.

In the end, one of the biggest challenges we face as an industry is that, thus far, not enough of the user base really makes decisions based on its privacy. That is a little less true of us, because we have a user base that I think has demonstrated, through using Firefox, that this is something it cares about. In the rest of the industry, that hasn't proven to be the case thus far, and we might be at a tipping point where it might be changing. I think we'd all like that to change.

However, regarding the incentives for a company such as Facebook, until Facebook users really demand something better, it's going to be hard for Facebook to deliver something better in terms of privacy. Our users do demand something better. They expect something better, and that allows us to deliver that.

Mr. Brian Masse: It's less about the capability than it is about everything else.

When working on microbead issues, one of the things we found right away was that a lot of companies wanted to do the right thing in terms of restricting the size of microbeads. Those are the small plastic additives to shampoo, toothpaste, and so forth. A lot of companies wanted to make the right decisions, but the regulatory body didn't provide a set of standard rules, which then allowed for the subsidization model to actually increase the profit margin at the expense of the environment. How do you compete in that environment?

In the same context, is the reluctance of companies to subscribe to the GDPR partly because, in moving toward that model, we have no enforcement of it? Some of them might say, in principle, "Yes, we're going to follow it", but the reality is that a lack of an incentive model would restrict their capabilities for third party source advertising, selling, data mining, and data management, which wouldn't make economic sense for them in that realm. Would others comply and fall in line if there was actually an enforcement model that made sure there was standardization?

● (1025)

Mr. Marshall Erwin: That's a useful way to think about it. What are the incentives that a company faces to get to a better place? Again, we have a user base that really cares about these issues. We have a model. We are a public benefit company. Those factors really anchor our decisions.

Your question is, what are the incentives that other companies are going to face? Again, there are two incentives that you can create that might not have existed thus far. One, if users demand it, that's going to change the incentives a lot. Two, if there is a regulatory regime, coupled with enforcement that actually has teeth, that's going to be something that companies will really pay attention to.

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

Mr. Brian Masse: Lastly, with regard to Firefox in particular, you've articulated that the development, the implementation, and the corporate culture around that element are what grounds it in terms of protecting privacy, and it's actually rated fairly well for those things. I want to be clear on this: It could be altered at any time should somebody else purchase Firefox or decide to go in a different direction, or whatever. It's a chosen direction of company policy and culture to provide the service in the way it does now, versus out of technological capabilities.

Is that correct?

Mr. Marshall Erwin: Again, there are a number of factors that ground our approach. Your question is, how easy is it to change those?

Mr. Brian Masse: You're good at summarizing.

Mr. Marshall Erwin: Some are simply a matter of policy; others are a matter of law. The corporate culture piece is remarkably difficult to change. It's not easy. Mozilla has two decades now of commitment to that culture. Even if we wanted to, it would not be a marginal effort to change the company's thinking on this. That's good. That's the way we like it, and we have a user base that really cares. That's actually the most critical incentive we face, the fact that this is a commitment that our users know we've made and they hold us accountable to that.

Mr. Brian Masse: Void of that commitment—

Sorry, I don't know if I have any time left.

The Chair: You have 30 seconds.

Mr. Brian Masse: The most important part of your testimony was that you noted the default settings and decided not to exploit that. You had the capability to do so, but you chose not to.

Is that correct?

Mr. Marshall Erwin: Do you mean the default settings in the Firefox browser?

Mr. Brian Masse: You said at the beginning of your testimony that you noted that there were some open default settings that you could have taken advantage of with the data breach, and you decided not to.

Mr. Marshall Erwin: More generally, we were looking at the default settings. The reason we paused our advertising was that we looked at the default settings provided to third party developers. We said that these were simply not accurate and the default seemed to provide data to those developers. That was a judgment we made about the Facebook platform. We were not in a position to collect that data, ever. It was not a question of whether we should access that data or not; it was just a question of whether the approach that Facebook was taking for its users was the right one.

● (1030)

Mr. Brian Masse: Thank you.

The Chair: Thank you, Mr. Masse.

Mr. Erwin, I especially want to thank you for your testimony this morning, and I appreciate your trip out here.

Mr. Marshall Erwin: Thank you.

The Chair: We'll suspend again for just a few minutes until our guests exit, and then we'll go in camera and talk committee business for about 15 minutes.

[*Proceedings continue in camera*]