HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 106 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, May 10, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 10, 2018

● (0845)

[*English*]

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

This morning we have it broken out into two hours. United Kingdom Information Commissioner, Ms. Denham, is with us via teleconference. We also have, from the Office of the Information and Privacy Commissioner for British Columbia, Mr. McEvoy.

We'll start off with Ms. Denham.

Ms. Elizabeth Denham (Information Commissioner, United Kingdom Information Commissioner's Office): Good morning, and hello from Manchester.

Thank you, Chair and committee, for the invitation to appear before you today.

I'm the Information Commissioner of the United Kingdom. I regulate data protection and freedom of information as well as a host of other personal information-related legislation.

I'm pleased to have the opportunity to speak to you today about the work of my office in investigating the use of personal data for political campaigning purposes.

I've watched some of the earlier sessions of your inquiry with great interest, and based on that, I need to set out something clearly at the outset.

In the U.K. and across the EU, information about individuals' political opinions is considered a particularly sensitive category of personal data to which additional safeguards under data protection law are applied. What that means, therefore, is that political parties and campaigns are subject to a combination of data protection, direct marketing, and electoral law when engaging in processing of data for electoral purposes with oversight by my office and the electoral commission. This has always been the case since data protection legislation was first introduced more than two decades ago, and it's simply accepted as a cultural norm.

These rules are there to ensure free and fair elections, and they do not undermine democratic engagement in the U.K. Instead, political parties have to engage with voters in a manner consistent with that law. Recognizing the special place of political parties in a democratic society, they've been given special status under U.K. data protection law to allow parties to carry out their campaigning activity.

In my complaint-handling role, I consider complaints from individuals against political parties when they think that their data has been misused. The number of complaints has never been particularly high. Other than a spike at election time, political parties have not, in the main, been a sector generating a high proportion of complaints. My office has maintained an ongoing dialogue with parties, meeting with them regularly and issuing bespoke guidance on how they can comply with the law when they are campaigning.

However, the EU referendum in the U.K. in June 2016 was an unusual exercise by British norms. Instead of being fought by established political parties, the referendum was led by campaign groups that were, in some cases, fuzzily constituted coalitions of like-minded bodies. The U.K. law on data protection is written to take account of political parties, but in a country where few referendums take place, the law has less to say about non-party campaign groups. This is made, considering potential breaches of the law during the referendum campaign, more challenging for my office.

We were concerned about some of the campaigning practices that we heard about and the provenance of the personal data used by campaign groups to target individuals. That's why in May 2017, I announced a formal investigation into the use of data analytics for political purposes. The original goal of the investigation was to pull back the curtain on how personal information was used in modern political campaigns.

At its heart, data protection law requires organizations to process data fairly and transparently, but rapid social and technological developments in the use of big data means that there's limited knowledge of or transparency around data processing techniques, including analysis, algorithms, data matching, and profiling to micro-target consumers and voters.

I think these techniques are attractive to political parties in campaigns as it enables them to target individual voters with messages in keeping with their political interests and values, but this isn't a new game played by different rules. The law continues to apply whether campaigning is conducted offline or online.

● (0850)

My investigation now involves over 30 organizations, including political parties and campaigns, data companies, and social media platforms. Among those organizations is AggregateIQ, which was used by a number of U.K. campaign groups, a company that this committee has already heard from.

What we didn't expect at the outset of our investigation was to be looking at the what, when, how, why, who of a reported 87 million Facebook profiles alleged to have been mined by an academic and passed on to a U.K. political consultancy working on the U.S. 2016 election and other political campaigns, plus multiple other lines of inquiry that I can't talk about at this time. This naturally raised concerns both in the U.K. and abroad and officers of Facebook and Cambridge Analytica have been called to account in various national parliaments.

I'm sure you understand that I can't speak about the particulars of an active investigation. The investigation is progressing at pace. Enforcement activity is ongoing, so it wouldn't be appropriate for me to comment further.

What I can say, though, is a number of organizations have freely co-operated with our investigation. They've answered our questions and they've engaged with us. But others have attempted to undermine the inquiry by failing to provide comprehensive answers to our questions, refusing to co-operate altogether, or challenging the process. In these situations we've been forced to use our statutory powers to make formal demands for information.

Some of my lines of inquiry are more developed than others, but an update on the entire investigation will be provided in a report issued by my office in the coming weeks. Whilst my colleague, Commissioner Therrien, is conducting his own investigation into Facebook, there are areas of joint interest that cut across both of our investigations. As Commissioner Therrien noted, the ICO and the OPC have a co-operative relationship and we can share information if it's necessary for our investigative purposes in the public interest.

When I think about your committee's work, I can see two distinct lines of inquiry: first, the immediate concern of Facebook, AggregateIQ, and others and whether existing laws in Canada have been broken, and then a second longer-term line of inquiry, a wider consideration of public expectations of the use of their data in the political context and whether the law needs to be changed. This inquiry is rightly looking not just at data protection law but also at other areas, such as electoral law, to see how these issues can be addressed.

I mentioned my report to be published in the coming weeks. I will be making findings as to whether individuals' rights were infringed, but I'll also be making policy recommendations on how the U.K. government and others could address the failings that I've uncovered, including greater transparency in political campaigning. While every jurisdiction is different, there may be some relevant lessons that could be read across into the Canadian context.

To put my cards on the table, and I say that against a backdrop of fully recognizing the public interest of political parties being able to communicate with voters, which is of course a cornerstone of democratic engagement, I believe that the use of individuals' data by political parties needs to be addressed in Canadian law. Canadians should be able to bring a complaint to an independent regulator.

The law that we have in the U.K. is built on sound foundations and principles and doesn't unnecessarily fetter the democratic process. In the U.K.'s data protection law, political parties have a legal justification for processing the personal data of individuals when carried out for electoral purposes.

● (0855)

My office is only part of the oversight picture in the U.K. The U.K.'s Electoral Commission is responsible for overseeing elections and political spending. Where there is crossover, my office can work with the Electoral Commission or decide which body should take the lead.

This is not to say that everything about the U.K.'s data protection regime is perfect. I said the system works for political parties, and it largely does. The Brexit referendum was a different beast, as I noted earlier. Non-traditional campaign groups either unfamiliar or unconcerned with data protection law may have crossed that line into unlawful activity, and I think the temporary nature of those groups has made pursuing them for the failures of data protection law more challenging.

The U.K. law already equips me with recourse to criminal sanction if a notice from my office goes unanswered. This means that even if a campaign group or an organization winds itself up, I can still have recourse to pursue individual former officers of that group. This might seem like a lot of powers for one body to hold, but as a regulator, I'm answerable to Parliament and I must be able to justify how I go about using my regulatory tools. I think the ICO has always been a proportionate and responsible regulator, and never more so than in the context of political campaigning where we are acutely aware of the inherent public interest in democratic engagement. This approach will continue under the GDPR and the new U.K. data protection bill when it's enacted.

The manipulation of voters via micro-targeting risks undermining our democratic model, and isn't that a major concern for all of us?

Thank you very much. I look forward to answering any questions you may have.

● (0900)

The Chair: Thank you, Ms. Denham.

We'll move over to Mr. McEvoy.

Go ahead.

Mr. Michael McEvoy (Commissioner, Office of the Information and Privacy Commissioner for British Columbia): Good morning, Chair, and thank you very much to the committee for the invitation to appear this morning, particularly alongside—it's a great pleasure—my colleague Commissioner Denham from the U.K. In fact, only a few short weeks ago, I was in the U.K. assisting Commissioner Denham with the investigation to which she made reference.

It wasn't long after my return to British Columbia that I was conferring with Commissioner Therrien at the Office of the Privacy Commissioner of Canada agreeing to jointly conduct an investigation into Facebook and the B.C. company, AggregateIQ, a company with which this committee is very familiar. That investigation continues. Of course, I'm not at liberty to disclose much about it until our work is complete in that regard.

What I would like to do this morning is pick up on themes referenced by Commissioner Denham that relate to the broad aspects of your committee's mandate. I'm referring to seeking out legislative remedies that will help assure Canadians of the privacy of their data and the integrity of our democratic and electoral processes.

Beyond investigating companies like Facebook and Cambridge Analytica, which are critical inquiries to be sure, it is also important for Canada's political parties themselves to take some measures for restoring confidence in the democratic processes in our country. I would invite you, as my colleague Commissioner Therrien has, to subject yourselves to accountability measures regarding the way in which you collect and use the information of Canadian voters.

A question worth pondering, I think, is whether the Cambridge Analytica scandal would have happened were it not for the increasing demands on political parties to gather and analyze personal data in the hopes of understanding it and using it to persuade voters. Democracy requires the citizenry to have trust and confidence in the political process, and a significant element of that process concerns how political parties collect and use the personal information that belongs to Canadians.

Parliament and some provincial legislators have created offices that oversee the collection and use of personal information by private and public bodies. Curiously, that oversight, with few exceptions, does not apply to political parties. British Columbia is an exception. B.C.'s Personal Information Protection Act, or PIPA, applies to all organizations in B.C. It is substantially similar to PIPEDA and for that reason generally supplants PIPEDA's authority in my province.

Political parties in my province have been subject to PIPA since its enactment in 2004. In the 14 years that have since passed, I can assure you that democracy has continued to thrive unimpeded in British Columbia. We have not heard concerns or suggestions that laws protecting the personal information of voters restricts the ability of political parties or candidates to engage voters.

Political parties in B.C. can and do collect personal information about voters, but they do so under the same reasonable legal responsibilities and obligations that apply to other organizations.

Generally, this means political parties get information with the consent of voters accompanied by a clear explanation of how and for what purpose that information will be used. I used the words "generally" and "with consent" because there are legislative provisions that allow parties to collect information without consent, specifically to get the voters list and other voter data from Elections BC. These provisions, however, come with a condition that the party receiving the information must provide a satisfactory privacy policy to the Chief Electoral Officer.

PIPA also gives citizens the legal right to request and correct the personal information that political parties collect from them and to register a complaint if necessary. These complaints are adjudicated by my office. A citizen's right to exert control over their personal information is a fundamental principle of privacy law. It is a principle strengthened by the EU's general data protection regulation, which Commissioner Denham just made reference to, and which comes into effect in Europe in just a few days.

You may be interested to know that my office is now undertaking a broad investigation of how the elected parties in our legislature collect and use voters' personal information. Those parties, I would note, have fully co-operated with our office's investigation. I expect that the investigation will result in recommendations and guidance that will help parties improve their privacy practices.

Of course, I know that recent proposed amendments to the Canada Elections Act will require political parties to adopt a policy to protect personal information and to provide it to the Chief Electoral Officer. These proposals are only a minimal step forward. They attempt to address the principle of transparency, but that is only one element of a proper data protection regime.

● (0905)

The proposed amendments do not require parties to respond to a voter's request for the information the party holds about them, nor does it allow a voter the right to ask a party to correct inaccurate information about them. Perhaps most important, there is no provision for an impartial third party to hear and determine a voter complaint. These basic legal standards have been a part of British Columbia law for years and are the norm in many western democracies. There should be nothing for political parties to fear in any of these legal obligations. In fact, implementation will do nothing but enhance the confidence of citizens in their democratic institutions.

With that, Mr. Chair, we are happy to take any questions you may have.

The Chair: All are aware on the committee that we're going to have a certain amount of time to ask public questions, and then after the first five-minute round of questions, we're going to move in camera, so just be prepared for that.

We'll start with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning to both of you. Good afternoon, I guess, in England. Thank you very much for joining us.

Mr. McEvoy, I'll start with you.

The BBC reported a couple of weeks ago that they tried to visit the offices of AIQ in Victoria. They found the offices pretty desolate, with a couple of people working there. Has your office attempted to contact AIQ principals who were involved or tried to visit the office in any way?

Mr. Michael McEvoy: The answer is yes, we are well engaged with AggregateIQ at this point. Beyond that, I don't want to say much. We are far from complete in our questioning of AggregateIQ.

I think perhaps I will just leave it at that.

Mr. Raj Saini: Okay.

Ms. Denham, I have a couple of questions for you.

There is one thing that concerns me that's occurring in England right now. Cambridge Analytica has declared bankruptcy, and the company that has emerged from that is Emerdata. There's another company called Firecrest Technologies. It seems the same actors are now realigning themselves. You tried to get a warrant, and I think you applied for it under Blighty's data protection law. They had seven days to argue against the warrant. They knew that your office was investigating or would come after them.

When you talk about a company, whether it be a retail outfit or a manufacturing outfit, if you move the physical assets of that company somewhere else, there's some accountability, because you can see a desk being moved, machinery being moved, product being moved. But you're talking about data now. Data can be moved very quickly. It can be taken some other place; it can be used in another fashion. If a company is going to restart itself, it needs product, and their product is data.

Do you feel the situation has come to the point where it may be difficult now to trace where that data actually went, knowing that the companies have realigned themselves in one way or another?

Ms. Elizabeth Denham: In regard to the comments on the warrant, I agree with you that the current provisions in our law don't allow us to move quickly with a warrant. We need to be able to respond to digital crimes and data crimes. The government has just tabled amendments that are going to give us new powers to be able to react more quickly and not have to give long notice periods to organizations. That said, we have been able to seize and secure a great deal of data from Cambridge Analytica, and we have executed two more warrants in this investigation, so we do have a great deal of information. If there are links between one company and another, and if their intellectual property and their data are being used by a new company, then we are able to investigate and continue our investigation. If a company is entering into insolvency, as in this case, then we are in touch with the administrators and we're able to proceed with enforcement action, both criminal and civil.

Mr. Raj Saini: As you're well aware, AIQ testified before our committee. Since that time, have they become more co-operative with your office?

Ms. Elizabeth Denham: We have recently received a letter from AIQ that opens the door to better co-operation than we have had. I don't know if that was a result of the testimony and the discussions with your committee; it remains to be seen. Actions will speak louder than words. If we don't receive co-operation, then as I said to my parliamentary committee in the U.K., I will seek other legal steps and actions.

● (0910)

Mr. Raj Saini: That leads to my final question. It's been reported in *The Guardian* that you are exploring legal options to have AIQ become more co-operative. Can you give any idea of what steps you may be taking?

Ms. Elizabeth Denham: I would rather not respond to that in the public domain, but I will say that we're also exploring options in co-operating with our Canadian colleagues in this investigation.

Mr. Raj Saini: How much time do I have left?

The Chair: You have 30 seconds.

Mr. Raj Saini: Thank you.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): I just have one quick question.

Our current Privacy Commissioner has not even close to the same powers that the two of you have. Do you think it's important, especially in a context of the Facebook and Cambridge Analytica scandal that our Privacy Commissioner has stronger enforcement powers, be it fining powers, leading to criminal sanctions perhaps, certainly over and above what he has right now?

The question is for both of you.

Ms. Elizabeth Denham: If I could start, I would say that the Canadian Privacy Commissioner's powers have fallen behind the rest of the world, so having order-making power, having the ability to levy administrative penalties, civil monetary penalties, and certainly the ability to seize material and to act quickly, I think are really important when we're dealing with global data companies and fast-paced investigations.

Even the powers that I have under the current U.K. Data Protection Act were not sufficient in this case. Government has moved really quickly and tabled amendments, which were passed last night, to provide us with even more powers of no notice inspections, streamlined warrants, the ability to make emergency orders, and also criminal sanctions for destruction of records and information.

That's important in the broader context with digital companies and being able to move quickly in the public interest.

The Chair: Mr. McEvoy, quickly.

Mr. Michael McEvoy: Our office is on record as supporting Parliament providing greater powers to the Office of the Privacy Commissioner of Canada.

It's really from the perspective of citizens that I think we need to think about this. Given the matters that you're investigating, Canadians want to have some sense that somebody with some regulatory power has their backs. That can't happen unless the regulator has the appropriate authority to ensure that these kinds of things are properly remedied if there is a concern with or a transgression of the law.

The Chair: Next up, for five minutes, is Monsieur Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair. I would like to thank both witnesses.

My first question is for Ms. Denham, but Mr. McEvoy may answer as well, if he wishes.

Madam Commissioner, you have drawn our attention to crimes related to the use of data and profiling.

The legislation seems to be unclear about the use of data taken from Facebook. Categories of people are created in order to target them with advertising or to influence them to vote one way or another. The argument made to justify the use of this data is that people voluntarily posted that information on their Facebook profile.

People voluntarily indicate on their profile that they are married, that they have children, or a red or blue car, for instance. These companies will ask what crime it is to categorize everyone who has a blue car. How can we say that a crime was committed in connection with the data or profiling if that information was only used to target people with a mere ad?

[*English*]

Ms. Elizabeth Denham: Under U.K. law, and in fact under data protection law across the EU, there has to be a specified purpose for the collection and the use of data. If, for example, somebody was answering a quiz and thinking that they were sharing that information for one purpose, such as academic research, and that data was then used for a different purpose, such as political campaigning or profiling an individual as to their categories and their political leanings, then that would be a contravention of U.K. law. That is precisely what we're investigating.

When somebody releases personal information in an application or on a social media site, there needs to be some notification and clear purposes as to what that information is going to be used for. If there isn't, there is a contravention of law.

At the beginning of my remarks, I said that when it comes to establishing political opinions or political persuasion, that's a special category of personal information that requires explicit consent to use, and that again is a question that's central to our investigation in the U.K.

● (0915)

Mr. Michael McEvoy: As you decide to share a certain amount of information with your friends that doesn't make it a free-for-all for the world. It is understandable, I think, for an individual using Facebook who expresses an interest in red cars might get an advertisement about red cars. What would certainly be beyond the expectation of an individual is that they would be psychologically profiled and identified as a candidate for a particular ad because they were open or neurotic or whatever the classification is. I think that goes well beyond what the expectation of an average citizen would be, and that does fall afoul of privacy law.

[*Translation*]

Mr. Jacques Gourde: Are there any studies or data proving that profiling is truly effective in certain situations and that it can change the course of history, or is it simply part of the political game nowadays? Perhaps we will have to legislate on that, but we will also have to work with profiling, because it has been done for about ten years now. It did not exist before. In the past, the approach was less methodical. Today, however, search engines and various digital tools can be used to conduct that kind of research.

How do you see the future, in light of this new reality?

[*English*]

Ms. Elizabeth Denham: When I speak to the political parties, and we've talked to all the main political parties and the campaigns in the U.K., I think what they're looking for, although they know that more research and perhaps more specific targeting can be done to reach potential and existing supporters, it could be that technologies have got away on us.

The principles of the law, the accountabilities, and the transparency are still really important to maintain the trust and confidence of voters. Just because we have new research methods, or just because people are arguing that these are more effective ways to reach potential voters and supporters doesn't make it right.

We need to look at whether there are some red lines here for the kind of back room, back office data matching and profiling that is possible in today's world. Now is the time to do it, because if we don't get the public policy right now, then we risk losing the confidence and trust of people down the road as these techniques become more effective and more freely available.

One of the recommendations in my report is going to be for a very specific enforceable code of conduct in the use of data analytics in the political context.

The Chair: Thank you, Mr. Gourde.

Next up for five minutes, we have Mr. Angus.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you very much for coming today.

Madam Denham, we had Mr. Massingham and Mr. Silvester come before our committee. Did you hear their testimony?

Ms. Elizabeth Denham: Yes, I did.

Mr. Charlie Angus: We were trying to determine the link between SCL and AggregateIQ. Mr. Massingham said there was absolutely no link, which seemed contrary to the documents we had obtained. Do you believe his testimony was forthcoming?

Ms. Elizabeth Denham: We have asked some very specific questions of AggregateIQ in the context of our investigation, and, as I said earlier to your colleague, and as I've said in public, we're still waiting for comprehensive answers.

We're also looking at a lot of material that has been provided to our investigation: witness statements, information from whistle-blowers, and documentation before us. That is one of the questions our investigation is focused on. We're hoping to get to the bottom of that.

● (0920)

Mr. Charlie Angus: Thank you.

Mr. McEvoy, you seemed to be very determined that political parties come under PIPEDA. We as politicians don't tend to talk about our data very much. We're very protective of it.

When I was elected, I found out that my main job is in my riding. We deal with immigration, with people coming to us with bankruptcies. People come to us with medical problems, deportation issues, child welfare. We gather an enormous amount of very personal information. Nobody trained my office on gathering it. We have a strict code. I assume most MPs' offices do. I've dealt with other offices in other parties about certain sensitive cases. It has always been very professional, but we gather that data to deal with constituents. We always have a separate file or a separate dataset for elections, but there's nothing to say that those couldn't be mixed up if we don't have certain laws or certain outliers. Do you believe it would be better to have the confidence of the people who come to us for service to know we are under a federal data law to protect privacy?

Mr. Michael McEvoy: It is important that Canadians understand that their data is being protected properly and appropriately.

I would draw something of a distinction. You talked about, essentially, the work you do for your constituents. In British Columbia that information would be, for the most part, exempt under freedom of information law.

Mr. Charlie Angus: Yes.

Mr. Michael McEvoy: What we're talking about here is political party activity and collection of data.

Maybe another way of answering your question, in thinking about this, is in British Columbia we have had occasion to investigate instances where, in the governing party's collecting information, there were allegations that it may have crossed a line, a grey zone, where that information moved, potentially or allegedly, from a government collection to party sources.

Without our ability to investigate parties, that investigation would have been stopped at that door, which I think would have been not just problematic in terms of our own investigation, but also in terms of the public understanding of what had truly happened to the information that was collected. Because we have a law that allows us to look at parties, we were able to look at that matter holistically and come to conclusions about what had actually happened to the data. I think that enhanced the public's confidence that data was being handled properly, and where it wasn't, that sanctions were available for our office to bring down.

Mr. Charlie Angus: Yes, I think it's important. Again, certainly in the work that we do in our MPs' offices, we treat that data very.... It's sacred. I always say to my staff, whatever's said in here is like being in the confessional: it could never, ever be put out there. We need to have that confidence. People come to us and share very intimate details of their lives, and then three weeks later we're calling them on the phone, trying to get them to take an election sign. They have to know that we are not using their personal data to get those election signs, but that's an honour code.

Would it be better if we had a very clear legal code so that, in an age when people are losing trust in politicians, they could say that in Canada they can trust that when they come and they share data, that data they want to share with us politically is being shared and the data they don't want being shared is not being shared?

Mr. Michael McEvoy: That's an interesting example you raised. If there was an allegation that somehow the data was leaking to the political party, as you describe it, the ability of a regulator.... I think the public's confidence would be enhanced in the system if they knew that there was some ability to investigate that to determine whether or not the party had improperly collected information that they shouldn't have. Again, it's for legislators to determine where that oversight power would be in Canada. I know there are some constitutional, legal issues with the OPC. In British Columbia there are occasions where my office actually has carriage over certain matters that are not necessarily squarely within our statute but can be referred to our office for adjudication.

Similarly, on whether there is an appropriate place, an appropriate piece of legislation, where privacy and data protection as it applies to political parties...perhaps it's not PIPEDA, I don't know, and again, that's for legislators to determine. However, you have the Privacy Commissioner of Canada who could adjudicate those matters, potentially, because he is in a good place. He has the expertise. He has the staff. He has the investigatory capability to look at those kinds of issues.

● (0925)

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

The last five minutes go to Mr. Baylis.

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

Thank you, Ms. Denham, for being here.

Obviously, as Canadian legislators and Canadian citizens, we have a concern about AIQ. It starts there for us because we don't want people using Canada as a barrier to conduct illegal activities somewhere else. We've had them in front of our committee. As you've seen, we've come to the conclusion that they were not forthcoming with us. I could speculate that they might have even been purposely trying to mislead us. They're part of a group of companies. They're part of Cambridge Analytica, SCL.... They were at one time called SCL Canada.

Also, it starts with Aleksandr Kogan and Global Science Research. This is the person who amassed all this data. Has he broken any of your laws? Have you made any determination on that yet?

Ms. Elizabeth Denham: We are looking at Dr. Kogan. We are looking at his app. We are looking at the operation of it, his relationship with Cambridge Analytica, and what actually happened on the ground with that app.

Dr. Kogan has refused to speak to our investigation, so again, we are proceeding with other options in trying to get a statement from him. Again, we have enforcement tools. We have civil remedies that we can pursue, but it certainly is an important line of inquiry for our investigation in the U.K.

Mr. Frank Baylis: I'm not surprised that Dr. Kogan is not co-operating. Let's assume Dr. Kogan has gone and taken this data. We would call this stealing, when you go in through the back door, take something that doesn't belong to you, and it's against the rules. I'm going to say Dr. Kogan has stolen this information.

The question becomes, why would Mr. Steve Bannon go all the way from the United States to Europe, to the U.K., and engage SCL and help start Cambridge Analytica? Did they have any specific abilities, or was it simply that they had access to this data?

Have you spoken to Mr. Bannon? Are you planning to speak to him as part of your investigation?

Ms. Elizabeth Denham: Again, I can't speak to that line of inquiry because of the ongoing nature of this investigation. I don't want to offer a hypothesis as to why the company was set up in this way. It certainly is a question that parliamentary committees on both sides of the Atlantic are asking, as well as attorneys general, and other regulatory bodies.

Mr. Frank Baylis: It does seem very interesting because Facebook, Google, and a bunch of these very powerful, capable companies exist and work in the United States, but they felt it necessary to go to the U.K. The one place they show up is the one place that has access to this data that Mr. Kogan has put together, and he is refusing to co-operate on how he got it.

We come back to Mr. Kogan, who has been financed in the past, in my understanding, by the Russian government and arms of the Russian government. We see the Russian regime under Vladimir Putin interfering in elections. Is it possible that Mr. Bannon went there to test run on the Brexit vote what he was planning to do six or seven months later with the American election? Is this a possibility?

Ms. Elizabeth Denham: I can say the focus of our investigation is about the collection, use, and alleged misuse of personal data in the context of Cambridge Analytica and SCL Elections. It's for others to make those connections internationally.

We will get to the bottom of the questions we have in our specific lines of inquiry under the data protection law in the U.K.

Mr. Frank Baylis: You have been very helpful, and we've been coordinating with the U.K.'s investigation as well. Has anybody from the American government contacted you to help coordinate what you're doing, and follow along the same lines as we are?

● (0930)

Ms. Elizabeth Denham: We have been in touch with our American counterparts in this inquiry. I have not been in touch with Congress or with politicians in this inquiry. That might be a question for Damian Collins and the DCMS committee in the U.K.

Mr. Frank Baylis: It seems to me there have been players in the U.K. who have coordinated or worked with a hostile foreign power —and by that I mean by Mr. Vladimir Putin's regime—to actively undermine your democracy. In the old days we would call that treason, and these people would be dealt with accordingly.

If you find these links, is this something you are going to pass on to that level?

Ms. Elizabeth Denham: Under my law, I have the ability to pass information to other law enforcement authorities or regulatory authorities if I deem it to be in the public interest to do so.

For example, I have passed information to the U.K. Electoral Commission that I thought was relevant to their inquiries about campaign financing. I can do that. If I found other information that would be pertinent to a law enforcement investigation, then I have the ability, in my law, to share that information.

The Chair: Thank you, Mr. Baylis.

Before we move in camera, I want to thank you for your co-operation from our committee's perspective and look forward to ongoing co-operation to that effect. We are also exploring all legal options for what this committee can pursue if problems arise from testimony at our committee.

● (Pause) ●

● (0955)

The Chair: I call the meeting back to order. My apologies for the quick changeover and the limited time to get settled.

I especially want to thank our witnesses today. Colin McKay is Head of Public Policy and Government Relations for Google Canada. We've met before. From the Council of Canadian Innovators, we have Mr. Jim Balsillie.

Welcome.

Due to our limited time, opening statements are five minutes.

We'll start off with Mr. McKay from Google.Thank you.

Mr. Colin McKay (Head, Public Policy and Government Relations, Google Canada): Mr. Chair, and members of the committee, thank you for the invitation to appear today. It's a pleasure to be speaking with you again about these important topics.

I'd also like to acknowledge that today is a particularly emotional day for Parliament. I had the good luck to spend time with Gord Brown both on and off the Hill, and I know he will be missed.

Google works hard to provide choice, transparency, control, and security for our users, and we appreciate the opportunity to tell you about how we protect Canadians and our billions of users around the world. I thought it might be a helpful context for this conversation to quickly touch on Google's presence in Canada.

For a company that is just 20 years old, we have some deep Canadian roots. Sixteen years ago, Google selected Canada as the location of its first international office. Since then, we have steadily grown to over a thousand employees in Canada, with over 600 programmers and AI researchers in Montreal, Waterloo, and Toronto. Our mission is to organize the world's information and make it universally accessible and useful. Google services provide real benefits to Canadians, whether it's Search, Maps, Translate, Gmail, Android, Cloud, or our hardware devices, our products help people get answers, organize their information, and stay connected.

Our advertising products help Canadian businesses connect with customers around the globe, and our search tools help Canadians find information, answers, and even jobs. Just a few weeks ago, we rolled out new ways for Canadians to find jobs using Google Search.

As you may know, Google has invested significantly in Canada's burgeoning artificial intelligence ecosystem, not only through the funding of organizations like MILA in Montreal and Vector in Toronto, but also by establishing research labs that have helped Canada attract and retain world-leading talent.

Our engineers work on significant products like Gmail, the Chrome browser, and Cloud, products used by billions of people around the world. We have a Canadian team developing safe browsing technology that prevents malware attacks and phishing scams, keeping the open web safe and secure.

This brings me to how Google has long thought about privacy and security. Google has been investing in tools and teams over the past five years to provide users with industry-leading transparency, choice, and security regarding their data. We offer tools such as My Account, Security Checkup, Privacy Checkup, Takeout, Google Play Protect, and more, all with the aim of protecting users' data, allowing users to make easy and informed privacy decisions, and affording users the opportunity to easily take their data with them to other platforms.

In 2015, we launched My Account, or myaccount.google.com, which provides Canadian users with quick access to a centralized, easy-to-use tool to help manage their privacy and security. This is used extensively. There were over two billion visits globally to this tool in 2017, including tens of millions by Canadians. While we continue to promote the use of this tool, it's clear that awareness is growing and that Canadians are using it to make informed choices.

Google promotes Privacy Checkup to users on a recurring basis so we can help our users keep their privacy choices up to date as their use of Google services changes over time. Users can see the types of data Google collects, review what personal information they're sharing, and adjust the types of ads they would like Google to show them. In addition, we have a tool called Security Checkup which helps users understand what devices and apps are accessing their data.

On our Google-licensed Android platforms, we've developed Google Play Protect, which monitors devices for potentially malicious apps. We design our products and implement product policies that prioritize user privacy. It's part of our commitment to ensuring our users understand how we use data to improve their experience with Google products and services. It's hard to keep data private if it's not secure, which is part of the reason we have built such a strong security team at Google. It's also why we have not only focused on the security of Google and our services, but have helped the entire Internet industry bolster security through our leadership with projects like Safe Browsing, HTTPS Everywhere, email encryption in transit, and our leadership on promoting two-factor authentication security keys.

We know that our users are people. They are family members, friends, and neighbours. Some are relying on our products to build their company, and they're non-profit. Others just need help finding a product, an address, or opening hours, but every one of them is putting their trust in us, and we recognize the enormous value of the trust Canadians put in us.

Thank you again for the opportunity to be here today, and I look forward to answering your questions.

● (1000)

The Chair: Thank you, Mr. McKay.

Next up, for five minutes, is Mr. Balsillie.

Mr. Jim Balsillie (Chair, Council of Canadian Innovators): Thank you.

Mr. Chairman, and committee members, I have closely followed your committee because I believe Canadians are facing the most important public policy issue of our time: data governance.

Canada's innovators know that data flows have transformed commerce and made data the most valuable asset in today's data-driven economy. Businesses use data to create as well as access new markets and to interact globally with both customers and suppliers. Control over data and networks allows dominant firms to hinder competition and extract monopoly rents from their customers and to deceive consumers via their data collection strategies. Vast troves of data are collected and controlled by foreign unregulated digital infrastructures. This is why the Council of Canadian Innovators called on our governments to design a national data strategy to ensure that cross-border data and information flows serve the interests of Canada's economy.

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

While the Facebook scandals instigated the recent set of testimonies before this committee, I urge you to arm yourself with the facts about the data-driven economy, which is completely different from the knowledge-based economy that proceeded it and the production-based economy of the 20th century.

Intangible commodified data does not function the same way as tangible goods. The data-driven economy gets its value from harvesting, identification, commodification, and then use of data flows.

What we have heard from companies such as Facebook, including at this committee, is an inaccurate picture of what is happening. The Cambridge Analytica and Facebook scandal is not a privacy breach, nor is it a corporate governance issue. It's not even a trust issue. It's a business model issue based on exploiting current gaps in Canada data governance laws.

Facebook and Google are companies built exclusively on the principle of mass surveillance. Their revenues come from collecting and selling all sorts of personal data, in some instances without a moral conscience. For example, in Australia, Facebook was caught selling access to suicidal and vulnerable children.

Surveillance capitalism is the most powerful market force today, which is why the six most valuable companies are all data driven. Their unique dynamics require a made-for-Canada strategic and sovereign policy approach, because data and intellectual property are now key determinants of prosperity, well-being, security, and values.

Data underpins all aspects of our lives, as you can see from the illustration I gave you as a framework. As an intangible asset, data has critical non-commercial effects. With this in mind, I make the following recommendation: implement GDPR-like provisions for Canada. GDPR offers valuable lessons and a point of departure for Canada's legislators and regulators. It is a universally acknowledged advance in privacy protection and control of data.

European policy-makers recognize that whoever controls the data controls who and what interacts with that data, today and into the future. This is why they ensured that EU citizens own and control their data. Similarly, Canadians should own and control their data. Canadians need to be formally empowered in this new type of economy, because it affects our entire lives. For our democracy, security, and economy, Canadian citizens, not unaccountable multinational tech giants, need to control the data that we and our institutions generate.

By focusing only on individual privacy, Canadians can find themselves plugging just one of many holes, which is, in effect, plugging nothing. We need a horizontal lens to legislation and policies. Privacy and digital public and private services aren't opposing forces. For example, Estonia shows that better data governance leads to increased privacy in digital services.

Economists consistently show that the data-driven economy is unfolding at a speed that outpaces the creation of evidence-based policy-making. I urge you to work with Canadian innovators and experts who understand open technologies, data sciences, competition, standard-setting, strategic regulations, trade agreements, algorithm ethics, IP, and data governance.

● (1005)

We need them to help craft detailed policies that are technical in nature. By working with experts, we can advance our country and ensure Canada doesn't miss participating in the data-driven economy, like it missed prospering in the knowledge-based economy over the past 20 years.

On a personal level, as a Canadian, I am deeply worried about the effect mass surveillance-driven companies have on both Canadian society and individual Canadians. Personal information has already been used as a potent tool to manipulate individuals, social relationships, and autonomy. Any data collected can be reprocessed, used, and analyzed in the future, in ways that are unanticipated at the time of collection. This has major implications for our freedom and democracy.

I am concerned that without the design and implementation of a national data strategy, our politicians are moving ahead with initiatives with foreign companies that are in the business of mass surveillance. Some of these companies have a proven track record of using data for manipulative purposes. Unfortunately, history offers sobering lessons about societies that practise mass surveillance.

It is the role of liberal democratic government to enhance liberty by protecting the private sphere. The private sphere is what makes us free people. There is no individual consent to, or opting out of, a city or a society that practises mass surveillance, and this is the path Canada is currently on. Therefore, in addition to putting in place appropriate economic incentive structures and regulatory frameworks, I also urge you and fellow elected officials to act boldly to preserve our liberal democratic values, to promote the public interest, and to assert our national sovereignty.

I thank you for considering my recommendations and for the opportunity to present here today.

● (1010)

The Chair: Thank you, both Colin and Mr. Balsillie, for your testimony.

We'll go to Monsieur Picard for seven minutes.

[*Translation*]

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

Mr. Balsillie made a few pointed remarks about Google, so I invite Mr. McKay to react to the allegations Mr. Balsillie made in his testimony.

[*English*]

Mr. Colin McKay: Mr. Balsillie has made some very constructive recommendations around the need for a data strategy for Canada, to enable Canadian businesses and businesses competing in Canada to understand the data they have at hand and the business opportunity that is presented to them by capitalizing upon that data. The government certainly has an opportunity to create a nuanced strategy that helps Canada differentiate itself from the rest of the world, not just in the tech sector but in health, where we already have quite a lead in terms of dealing with health information, as well as agriculture, mining, and manufacturing.

A data strategy does not need to be as restrictive or prescriptive as Mr. Balsillie has suggested. In fact, a strategy that tries to box Canada in or creates obligations that are not either parallel or similar to those available elsewhere in the world will actually limit the opportunities available to Canadians to innovate, both in Canada and internationally. There needs to be consistency and predictability in any regulatory framework that's set up.

On a final point, I'd just like to underline that despite what Mr. Balsillie said, we do not sell the personal information of our users. We've built a business model that delivers services and products to users, relying on a personal relationship that uses the information they share with us to provide personalized services for them.

We support that broad array of services that are provided free to Canadians and everyone else in the world through advertising. It's advertising that's targeted at aggregated groups, not at individuals, and there's no exchange of personal information between Google and advertisers. It's simply recognizing that there's an economic transaction that needs to happen to provide those services, and advertising is the most common and convenient way to deliver that right now.

[*Translation*]

Mr. Michel Picard: That is exactly what I am getting at.

I would like to see an approach that is not directed at insiders, but rather an approach in layman's terms, if I may say, so people or the general public who are following the committee's proceedings can understand.

To really understand all the ins and outs of all this entails, I will pick up on what you said last. Let's try to have a discussion that focuses exclusively on the commercial aspect and not on broad policies and broad philosophical concepts.

When someone registers with Google, they do not have to fill out a special form, do they?

Mr. Colin McKay: Are you talking about a special form for the services offered by Google?

Mr. Michel Picard: I do not have to fill out a form that includes various personal information in order to use the Google browser.

● (1015)

Mr. Colin McKay: No.

Mr. Michel Picard: Since you have little or no information about me, my first reaction is that there is no information about me that could be at risk.

Mr. Colin McKay: That is true.

There are levels of expertise related to individuals. If you register for a service offered by Google, you are given the service and it is assumed you are a man of a certain age who works in Ottawa. When you use our service, we can see what you do with the search results about a hockey game, for instance. While you are using the service, we make assumptions about your preferences and what you frequently search for.

Mr. Michel Picard: Okay.

The fact that I prefer a type of book or a sports site, for instance, is that not a personal preference that becomes private information? Unbeknownst to the user, their use of the browser is recorded and assumptions are made about their behaviour.

If I understand this correctly, you turn to the private market and tell ad buyers that you have targets for them. Nice to provide a free service, but it does not pay the grocery bill at the end of the month.

[*English*]

Mr. Colin McKay: The point to make would be to distinguish that we don't provide a service that allows advertisers to target individuals. What we do say is that we have identified users who search for results for hockey games and might search for results for hockey games by a particular team or in a particular province.

[*Translation*]

Mr. Michel Picard: You provide the service of identifying the individual because you have the information from the IP address.

Mr. Colin McKay: We do not identify the individual.

[*English*]

For the advertiser, all we'd say is, “You would like to deliver an advertising campaign towards people who have these qualities. We will deliver that advertising campaign.” They do not know who is seeing the ads. They don't get information about who is seeing the ads. They have an idea of the number of people and the attributes of the people who have seen the ads.

Mr. Michel Picard: But you do know.

Mr. Colin McKay: We do that.

Mr. Michel Picard: You do that, but you do know who used that, because you have the IP address. You know the person related to the IP address, although you'd have to prove that the person who keyed in the information is the same one who is registered on the IP, but still there is no computer contacting any site. Someone does, and therefore you have in hand the missing link of personal information with any third party interest.

Mr. Colin McKay: I mentioned My Account. If you have an interest in understanding how we've used that information and how we've provided services to you, if you go to My Account, you can see a listing of those attributes and those qualities that we've associated with you. In terms of understanding what information we've exchanged in the course of our relationship, we make that clear in My Account.

It is not in our interest to engage in any type of transaction with a third party that exchanges that information. The exchange we have is that in the course of providing that information to you, we might learn more about your need to find parking near a hockey game because of your preference to go to hockey games. We will therefore, in Maps, tell you where the nearest available parking is.

Mr. Michel Picard: Thank you.

The Chair: Thank you, Mr. Picard.

Next up for seven minutes is Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde: Thank you, Mr. Chair.

My question is for Mr. McKay.

On Tuesday, Google announced that it will soon be possible to use artificial intelligence to converse on the phone in our place. That means that my Google virtual assistant will be able to make a hair appointment for me and record it in my personal agenda. I will simply have to ask it to do so.

What worries me about this is that, if it is possible to find information about a third party and enter it in someone's personal agenda, those same robots could ask a multitude of questions to 100,000 people. Do you like blue, for example. The robots could ask seven, eight, nine, ten, eleven or twelve questions, and then analyze the answers.

In terms of data, we are now in the wild west. It is changing so quickly. Companies like Google and Facebook can get personal information about people. After that, there will be a void. They will be able to do anything they want with the data, data that people voluntarily gave them.

With these tools, Google's strategy is to sell services and to give services to the public. How will you protect the data you can record? Can you use this kind of robot to get data that you will then resell to third parties later on?

● (1020)

[*English*]

Mr. Colin McKay: I'll start by replying to your last observation, which is we don't resell information, so that is not in consideration.

In speaking about the specific project Duplex that was discussed at our developer conference this week, that's a project. It hasn't rolled out into implementation. It's an attempt to explore how to provide you with a service. At the moment you can speak to your phone and ask for the phone number for a restaurant and then dial the restaurant and try to schedule an appointment. We're trying to explore how we can use artificial intelligence to get through the entire transaction of making a reservation for you.

That project Duplex is very limited in scope. I think three or four examples were provided during the conference. Those are the three or four examples that it can conduct. It's meant to provide a service to the individual. It's not meant to collect information. It's meant to be supplementary to the relationship we have with a Google user in terms of what information they are looking for to search, how they are trying to slot information into their calendar, and how they are trying to identify places to eat on Google Maps.

In terms of your question about broader surveys, that's not even under consideration right now. Broad-based surveys that drive voter interest or user interest are not something we conduct at the moment, so that wouldn't be an implementation of this tool.

I have to underline that this is using artificial intelligence in a way to conduct mundane tasks that provide a benefit to the user, provide time to them, and make that interaction as efficient as possible while providing a clear-cut service for the user.

[*Translation*]

Mr. Jacques Gourde: Mr. Balsillie, let's talk about all the data gathered by the big players in the world who directly or indirectly have access to our private life. If I use my virtual assistant to make a reservation at a restaurant, by the end of a year, Google will know that I go to Saint-Hubert every two weeks, for instance. It does not stop there. It will know where my favourite garage is and what kind of car I drive. That is a lot of data that can be reused. And yet, I provided it voluntarily by choosing a restaurant.

You said that we need a framework and legislation on the use of personal data, but how can we do that if that data is provided voluntarily? If I give my friends my personal phone number, it is because I want them to call me. Before the courts, the Web giants will say that the data they received was provided to them voluntarily. For instance, someone might post a picture of themselves on Facebook with red hair because they like to dye their hair red. There is nothing we can do to stop that.

What do you think?

[*English*]

Mr. Jim Balsillie: Thank you for your questions.

If I may, the first thing you have to understand as I go into this is that enormous amounts of data are collected without transparency, without your voluntarily knowing. What they've discovered with GDPR is that these social media platforms have literally millions of pages on you without your knowing it, including all the routing of where you personally moved throughout the year.

Many other things, different datasets, are brought together or “hashed” as they say. There are enormous sets of data that you haven't consented to being given. My main response to that is I'm encouraged by the questions you're asking because it shows me that you're not prepared to be tricked by platitudes like “informed consent” or “anonymization” or “transparency” or “nuance.” Those are trick words. Be very careful when they say they don't resell information because.... Do you exploit information? Understand that enormous amounts of data are collected without your knowing.

Have you heard of Sidewalk Labs? How are you able to opt out of all of that information they collect on you? There was a recent story of how Facebook was working with hospitals by anonymizing your data for your health care but were able to cross-reference that through AI to your personal social media and extract that to know who you are.

So, be very careful with these claims of informed consent and voluntariness in the surveillance state. As was said earlier, this is going much faster than we understand it and we are cascading towards a surveillance state. As you see by the framework I give to you, it touches all aspects of our sovereign citizenship, well beyond the economy.

● (1025)

[*Translation*]

Mr. Jacques Gourde: In years to come, will it be possible to have a private life, privacy, when all that data is being collected?

In five or ten years, will it still be possible to have a private life?

[*English*]

Mr. Jim Balsillie: It can, if we have responsible rules and regulations in society. This is what Europeans have had almost 10 years of debate and discussion on. They have discovered; they have come to a nuanced position. There's nothing extreme about GDPR in Europe. They figured out how they can be an open, innovative society as well as protect individual privacy and transparency to benefit their citizens. It is absolutely resolvable, but it takes responsible, expert, technical regulation, which is exactly what Europe spent nine years undertaking.

The Chair: Thank you, Monsieur Gourde.

Next up for seven minutes is Mr. Angus.

Mr. Charlie Angus: Thank you very much.

Mr. McKay, it's good to have you here, and Mr. Balsillie.

Mr. McKay, you talk about deep Canadian roots. You certainly have deep Canadian roots. In my region you compete against all our local newspapers for online advertising. Would you consider deepening your roots by paying the HST so we have a level playing field?

Mr. Colin McKay: I'll answer that in two stages. Number one, we provide ad technology services to newspapers, and we provide revenue—

Mr. Charlie Angus: Yes, but I don't care about that. Tell me, are you interested in paying the tax?

Mr. Colin McKay: I want to differentiate because your study is predicated on one company's behaviour. We provide services to newspapers that allow them to increase opportunities to gain revenue from their online viewers.

Your second question about GST, yes. If the government takes the steps to make GST applicable to a company in our situation and other online businesses, then we will take the steps, as we do in every other country, to collect it from our users who purchase things from us.

Mr. Charlie Angus: Is Minister Joly moving in that direction?

Mr. Colin McKay: I don't think it would be Minister Joly, would it? It would be Minister Morneau. It's up to the government to make that decision.

Mr. Charlie Angus: Up until now there's been talk about how you're not paying the HST, but then you also aren't being covered under section 19 of the Income Tax Act, which if you're not paying HST as a Canadian company, then why should people get a tax deduction for giving advertising? Google has called the questions about paying taxes on these issues of advertising punitive. Are you saying now it's not punitive, that it would be fair?

Mr. Colin McKay: Number one, we do pay tax on certain of our sales, like hardware and other elements of our sales in Canada.

Mr. Charlie Angus: Yes, I know. That's because you have to.

Mr. Colin McKay: All I'm saying to you is if the government makes moves to implement legislation that requires us and other online companies to collect HST on behalf of the government, then we will take the steps to comply with that.

Mr. Charlie Angus: Okay.

I notice in the U.K. in 2014 Google's tax was less than $7,000, which is about the average that a U.K. worker pays, and yet you paid out $534 million in bonuses. Your level playing field around the world works pretty well for you.

I want to get into this question about Google's philosophy. I was a big Google believer. When you guys started out I thought this was really awesome. I met Google in New York. I loved that philosophy, “Don't be evil”, but your founder also said that the Google policy on a lot of things is “to get right up to the creepy line and not cross it”.

Can we trust you to decide what's okay creepy, what's too creepy, and what's downright evil, when you're facing a class action lawsuit for illegal data collection? By using the loophole on the iPhone, you've been accused of tracking citizens in real time without their consent. You're facing charges in multiple states. Now there's a complaint about collecting personal information on children under 13 without their parental consent, including location, device identifiers, phone numbers, and their use across different websites. Rather than trusting you to decide what's creepy, shouldn't we just have legislation?

● (1030)

Mr. Colin McKay: That's why, in my opening remarks, I had a list of tools we have developed that are available to users. You're right. There needs to be transparency around what we're collecting and clarity around why we're collecting it and what benefit it has to the user. Over the years we've learned from our mistakes. We've learned from incidents such as the ones you've cited.

Mr. Charlie Angus: They're not mistakes. These are class action lawsuits. These are charges. If you guys get caught and then you learn lessons, this is the same thing we have from Facebook. If the public policy is to go right up to the creepy line, that doesn't give me much comfort.

Mr. Colin McKay: The public policy is not to reach a space that is uncomfortable for our users. The policy we have in product development is to develop leading-edge products that provide the greatest range of benefits for our users. There are different rates of adoption and different levels of comfort with adoption.

Mr. Charlie Angus: Thank you.

Mr. Balsillie, I'm really interested in this discussion on surveillance capitalism. I was deeply against the regulation of Google because I wanted to see it develop. Imagine, me a socialist, and here is an entrepreneur warning us about surveillance capitalism. We are living in an upside-down world.

What concerns me is that in Canada we see Google with their former policy director in the Minister of Canadian Heritage's office. In the United States, Google's patent director is now in the patent office. There are serious questions about the undermining of patent law in the United States by Google because of their enormous power. The Bank of Canada has warned about the power of companies like Google to undermine competitiveness. We see in the tech sector that patent lawyer Michael Shore has said that the U.S. is turning into a "banana republic", because legislators are rewriting the law to protect the interests of giants like Google. Meanwhile, the U.S. has dropped from first to 12th in global patent strength ratings over the last four years.

For Canada's tech sector, given the very close, comfy, cozy relationship between Google and the present government, where do you see us taking our tech sector in terms of innovation and building a credible relationship with Canadian consumers on issues of privacy?

Mr. Jim Balsillie: My greatest concern is that I know these partnerships were undertaken without an economic analysis domestically. Quite frankly, we don't know. I know as an entrepreneur that they have deeply negative spillover effects on our innovation outputs. You see that this year Canada slid behind Poland in innovation performance, so we're 22nd in the world, and Poland is 21. Once you're out of the top 20, you're not really considered a credible innovation nation. I would tie our performance directly to the fact that we have not created sovereign innovation positive spillover approaches.

To answer your question, I think we rush into these things. I'm directly aware that they're done with no economic analysis involving no experts on their spillovers. I can't imagine that a business would ever do a partnership without a business case analysis. I think the first thing we need to do is start analyzing the innovation effects of these varying partnerships or relationships and use proper economics, not "lobbynomics".

The second thing is that competition law and privacy law—as I mentioned regarding Estonia, and the EU is doing some very active competition strategies—work very nicely to the benefits of innovation and the economy and citizenship. They can all work positively together if we approach them with an understanding of their true nature.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

I was just talking with Jean-Denis. I'm going to push the meeting as close as we can to 11 a.m.. There's another meeting here at 11 a.m.

Without further ado, Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Mr. Balsillie, you indicated in your opening remarks that you categorized Facebook and Google together amongst other big data companies. Obviously, Facebook and Cambridge Analytica prompted this study, and it was pretty clear to me that sharing the amount of information with third party app developers as Facebook had been doing was contrary to our law. In fact, they were before us and said they didn't particularly agree with that assertion. They did say, though, that it was certainly not appropriate, and they've changed their practices.

Mr. Balsillie, you've put Google and Facebook in the same sentence. Are there particular practices Google is undertaking right now that you would say should be changed, and if so, why?

● (1035)

Mr. Jim Balsillie: I think there are many practices that should be changed.

One, you have to look at the ethics of the algorithms and how they impact and persuade people's behaviour. You had comments about advertising, and there's been considerable discussion about how algorithms promote certain kinds of divisive viewing on things like YouTube, because the algorithms are designed to get you to watch more, and they nudge you more to extremes the more you watch.

I think we have to properly regulate these things. I think we need proper standards for them. I think you've learned that companies respond after they get caught, and this shows that you need proper and responsible regulation.

It's not the same but it rhymes, in that we heard a lot of these issues in California when they started to legislate for emissions on cars and everybody said that it would be the end of the automotive industry, that you couldn't innovate, and that it wasn't going to be profitable. We now have better cars, less emissions, and record profits from the automotive companies. These things, properly implemented, can all positively reinforce one another. I think there's a very positive societal and capitalist way forward here.

Mr. Nathaniel Erskine-Smith: Mr. McKay, I have my Google Ads Settings open. There are 59 things I apparently like. Some are correct. I don't particularly like running and walking, but I do like action films. Having said that, though, these 59 things aren't necessarily why I'm being targeted. You have where I've been with my phone for the last 12 months, from what I understand.

I'd be interested to know to what extent you're scraping words from my Hangouts and my emails. You have everything I've searched for on Google and you're checking every website that I visit on Chrome and what I've bookmarked and beyond that. It's not these 59 things I'm getting targeted for advertising. Why don't I see more? Why isn't there more transparency in these 59 things?

Mr. Colin McKay: If you dig into that tool, you'll see your location history. Your location history is something that you explicitly signed into when you were setting up your phone. You have the ability to go into your phone and both turn off the location history as a whole for all the services—

Mr. Nathaniel Erskine-Smith: No, I understand that, because I did say to you I understood you knew where I was in the last 12 months.

My question is about the transparency of advertising. If I receive an ad, I'm not able to look under the hood to know what has specifically been used to get this ad to my screen right now as a consumer. Why not?

Mr. Colin McKay: If you're looking at specific parts of our advertising network, there is in fact a little reverse D that you can press on, and it will tell you why you saw that ad in our display network.

Mr. Nathaniel Erskine-Smith: Okay. Facebook used to have this, and, I think, has this now. They're going to have to get better at this, and perhaps you will too, because the explanation oftentimes is that you've liked similar things on the Internet.

Mr. Colin McKay: Yes.

Mr. Nathaniel Erskine-Smith: That can't possibly be the level of transparency that's acceptable, so how detailed is your transparency?

Mr. Colin McKay: Well, you've described it right there. You just called it up while we were talking, and you have 59 items, some of which are wrong. I have to tell you that for quite a few years the majority of Google thought I was a woman.

Mr. Nathaniel Erskine-Smith: It's not just the 59 items, right? It can't possibly be those 59 items, so it's everything I've searched on Google. It's my browser history. It's not just these 59 things. When I see an ad, I can't track everything, every reason that I've been targeted, that it's because I actually searched a website, or it's because I searched something on May 1. That I don't see, correct?

Mr. Colin McKay: You and I are speaking to a similar goal, which is, you're right. You should have the ability to understand how you're exchanging your information with us, and how we're using it to deliver services. We try to do that in a suite that we've developed, whether it's through My Account or through Privacy Checkup. Clearly, you're identifying a situation in which you're not getting all the information that helps you feel comfortable.

Mr. Nathaniel Erskine-Smith: Yes, because my worry is we had Rob Sherman before us who said that, yes, they didn't do what they should have done at the time. Three years from now, are you going to be sitting across from me saying, yes, you shouldn't have done what you did at the time? We have to regulate, but right now if you actually agree to transparency, you probably have to be more transparent than you are.

When it comes to emails and Hangouts, if I send an email saying, "Sorry, for your loss, and I hope to attend the funeral," or "Congratulations on having a baby," are the people I'm sending the information to going to start getting ads about funeral services or strollers?

Mr. Colin McKay: If they're using our products, no. We don't serve ads based on the content of your email or your Hangouts. All we do is search that content to make sure you're not seeing malware or experiencing a phishing attempt or some sort of breach to your personal security. We run automated systems to ensure the security of your account, but we're not serving ads based on the content of your Gmail in that particular specific way. Especially in the two contexts you just described—

● (1040)

Mr. Nathaniel Erskine-Smith: Tell me in what different way you are targeting the ads based on my email and Hangouts history.

Mr. Colin McKay: Well, in Hangouts you wouldn't be getting ads. In Gmail you get generalized ads based on the broad understanding of who we understand you as a user to be. It's not based on the content of the inbox or the mail, no.

Mr. Nathaniel Erskine-Smith: Okay.

The last question I have is about third party apps. We had app developers on the Facebook platform who were receiving troves of information that was completely unrelated and well beyond the scope of what they needed to deliver the app.

Walk me through your third party app sharing and the information you share with third party apps.

Mr. Colin McKay: Sure. We don't share any information with third party apps—

Mr. Nathaniel Erskine-Smith: No, but they do get access with basic account information—

Mr. Colin McKay: Yes, that's basic account information, so they get email address—

Mr. Nathaniel Erskine-Smith: What's in my basic account information?

Mr. Colin McKay: It's the email address and name. There's a third element, but it's not sensitive. It's those two pieces, and then you have to engage with a third party app developer to agree to provide—

Mr. Nathaniel Erskine-Smith: So there's no third party app that would receive anything beyond basic account information?

Mr. Colin McKay: There's no third party app developer, who without engaging with you in a specific conversation about consent to grant access to other information in some circumstances by you providing information to the app developer—

Mr. Nathaniel Erskine-Smith: But, that's up front, right? That's like.... I might not know what I'm agreeing to because the total information is not particularly disclosed to average consumers to say they're agreeing to *x*, *y*, and *z* and a whole bunch of information is going to get out the door.

Mr. Colin McKay: When you're installing an app on a licensed Android phone, you're given a specific menu that is required to have a link to a comprehensive and clear privacy policy so you understand their attitude towards privacy and security. Then it specifically identifies those elements of information that are either held or generated by the phone or by your account that they're requesting access to. On an app on Google Play for an Android phone, you have to be able to link through and see in greater detail why they want that information.

The Chair: Thank you, Mr. Erskine-Smith. I'd love to give you more time.

Next up is Mr. McCauley, for five minutes.

Mr. Kelly McCauley: That was fascinating information. Thank you, Mr. Erskine-Smith.

Mr. Balsillie, you talked about the EU's GDPR. Is there anything that you would change of that if Canada were to adopt something similar?

Mr. Jim Balsillie: Based on the core principles, no. The aspects that I'm zoning in on are, one, that you have personal ownership of your data and personal control over it, that you have awareness of what they're doing, and that you have what's called the right to delete and the right for portability.

The second thing, which we haven't had much discussion on, which is a very central part of the GDPR and this was a tremendous tug-of-war between Brussels and Washington over many years, is this element of safe harbour in routing. It is important to understand that no matter what we regulate in Canada, I've been told by experts that something akin to 80% and 90% of our data is routed through the U.S. Even if I sent you an email across this table, it's routing outside. It's called a boomerang effect. You have to understand that, per U.S. law, Canadian data has no rights whatsoever in the United States. You have no right to privacy; you have no right to anything. What the EU also did was manage the routing so that it never left the jurisdiction of what they prescribed as appropriate treatment of that data.

The GDPR is nuanced. It was the subject of many years of debate, from many perspectives. Using GDPR-like approaches is a minimum we should take in Canada, and then look at other forms of activities, such as the economic development opportunities for primary industries that Mr. McKay talked about, and many other aspects that we could extend beyond that.

It's also very important to remember, although it's not the purview of this committee, that in parallel the EU did a sustained set of studies and plans on competition behaviour for what's called the inherent asymmetry of data, where the big get bigger. If you want to promote economic advancement and prosperity, you also have to look at the competitive structures of that.

Competition and GDPR dance in harmony through pretty much a decade of work.

Mr. Kelly McCauley: That was my follow-up question. You talked about the value of data. My question was going to be, how do we monetize it in Canada but protect privacy. However, I'm going to move over to, what is the role of the monsters of Facebook and Google in Canada under the system where we want to monetize the value for Canadians and not just the big getting bigger?

● (1045)

Mr. Jim Balsillie: I don't see them as monsters. I just see them as capitalists.

Mr. Kelly McCauley: Sorry, giants.

Mr. Jim Balsillie: They're capitalists, and the job of a corporation is to do what a corporation is supposed to do and the job of government is to regulate. It is a complex issue because this is the biggest force in the history of capitalism, where six companies come from nowhere to be the most valuable companies in the world in a very short period of time. How they're managed in terms of competitive structures, and regulated, and how we do it for the benefit of Canada's economy and Canadian innovators is very important. Things such as competition behaviour and data ownership also must be woven in a national data strategy that looks at prosperity and many other things that go along with it: employment rules, cyber rules, and so on. This is a big file, and we need to urgently address it in a horizontal way as a nation, as policy-makers.

Mr. Kelly McCauley: We, this government, are not the fastest acting. If we were to approach GDPR, it could be years from now.

Things are moving so quickly. What should we be looking for, to adjust as we go, so that we're not introducing a GDPR for yesterday's rules or yesterday's reality?

Mr. Jim Balsillie: I think we have to reflect on the fact that they're nine years into this in Europe, and we're getting at it now. That wasn't necessary for this country. I think we have to reflect on being up to date, and involving experts.

I think you've had excellent testimony from folks like Commissioner Therrien on updating our privacy rules. I think you've had the Competition Bureau come in and talk about updated competition practices.

There has been a fair bit of work. I would encourage our legislators to actually embrace this, and say that 2018 is the year of regulating and legislating the data surveillance capitalism and the data-driven economy for the benefits of Canadians and Canadian citizens, for now and in the long term.

The Chair: Thank you, Mr. McCauley.

Next up, for five minutes, we have Mr. Baylis.

Mr. Frank Baylis: Thank you, Chair.

On the GDPR rules, I agree with Mr. Balsillie.

Would you say that these are the leading rules in the world right now which we should be looking to?

Mr. Jim Balsillie: They set the standard, yes.

Mr. Frank Baylis: They set the standard.

Mr. McKay, when the GDPR rules came into place, Facebook purposely moved a lot of their data from Ireland to outside the jurisdiction of the GDPR rules.

Has Google taken any such actions?

Mr. Colin McKay: No.

Mr. Frank Baylis: You must now have to look at complying with these GDPR rules. What actions are you taking to comply with them, if you've not taken actions to move away from them?

Mr. Colin McKay: We've been investing in the teams and improving our tools to comply with GDPR for a very long time. It's a tremendously complex challenge, even for a company of our size. It's an even greater challenge, not just for smaller companies, but for the privacy commissioners in Europe, themselves.

What we're doing is reflected in the tools I mentioned in my opening remarks. It's reflected in the sorts of permissions and control that individual users have across all of our services around the world.

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

Mr. Frank Baylis: So users around the world are going to benefit from the GDPR. Are you not going to have a two-tiered system?

Mr. Colin McKay: Users around the world are benefiting from a greater focus on trust, transparency, and individual control. That's a central baseline in the GDPR as well as other data protection regimes.

Mr. Frank Baylis: Let's be specific. Mr. Balsillie tells us that these rules are the best in class right now.

You're working very hard to adhere to those rules. You haven't moved data, as Facebook has, to avoid those rules. Those rules are going to be done. You've programmed for Europe. Is everybody else in the world going to benefit from those rules, or do we have to, as Mr. Balsillie suggested, put in our own rules and go back to Google and say that they had better adhere to the Canadian version of GDPR?

Mr. Colin McKay: I think if you're looking at what is the best in class, raises the most boats, standard for data protection obligations, then GDPR is setting that right now. It is driving change, both in our company and in other companies.

Equally, it's presenting a real challenge to companies that don't have sophisticated internal IT systems, or a clear understanding of what data they hold, and what responsibility they have to the users, especially companies that try to export or import from Europe, or have a relationship with customers in Europe. What we're going to see over the next six months and more is companies struggling to understand what their obligations are under GDPR.

● (1050)

Mr. Frank Baylis: If they're not as big as you, they're probably just going to have to adhere to them and say that everything they do adheres to GDPR—

Mr. Colin McKay: No, the challenge for them is actually—

Mr. Frank Baylis: I'm asking, is Google going to do that?

Mr. Colin McKay: Yes.

Mr. Frank Baylis: Is Google basically going to make sure that if someone has a transaction in Japan, or is talking from Canada, Japan, whatever, the rules that you put in place to meet GDPR are going to protect all of those other activities that are not actually touching Europe or being routed through Europe?

Mr. Colin McKay: They're going to see follow-on improvements and greater transparency control as a result of our compliance with GDPR.

Mr. Frank Baylis: Will they get the same? I'm sure they'll get better, but will they get the same as GDPR, or are you going to purposely triage and say that this one's going to be getting GDPR, and this one's not?

Mr. Colin McKay: We're not going to make explicit choices like that. What we do, as has come up in the conversation, is.... There is data protection and privacy legislation that varies from country to country. We need to meet the obligations in each country. What users are going to see is that the entirety of the controls and tools available to them are improving both as a result of our investment and the obligations of GDPR.

Mr. Frank Baylis: Has there actually been any data breaches from Google's databases compared to what's happened with Facebook?

Mr. Colin McKay: Not that we're aware of.

Mr. Frank Baylis: Okay.

You've said that you don't sell the data. I agree with you. Why sell it? You own it. It's totally valuable. Just rent it out and let people ask you for it. That's your model. Is that correct?

Mr. Colin McKay: We own the data that we have about you, and we use it to sell ads.

Mr. Frank Baylis: The reason someone stole the data from Facebook is that they said, “Why would I give you this data? I'm going to use it and sell the ads even to these bad actors. I'll use it. Why would I give it away?” Someone had to go in there and fake it and steal it.

Has anybody tried that? Is that happening to Google?

Mr. Colin McKay: Not that we've seen.

The Chair: Thank you, Mr. Baylis. We're right at the edge here.

Thank you to everybody—

Mr. Angus

Mr. Charlie Angus: Mr. Chair, because we were slightly condensed in this round because of the last round, and our two witnesses have provided us with an enormous amount of information, I'm wondering if it's possible to send them questions. We didn't get to questions like smart city, questions of moderating the Google Maps, and some of the questions on innovation.

I'm just wondering if it would be possible, through the chair, to follow up with questions so that we can make sure we've done all of our due diligence.

The Chair: Absolutely.

Are you okay with answering those questions when they come?

Mr. Colin McKay: I assume they'll be routed through the committee.

The Chair: Yes.

I just have one question for Mr. Balsillie, and I'm sorry, time is definitely up.

You mentioned the term “surveillance capitalism”. I guess the whole reason we're here today was started from a potential voter fraud somewhere across the water in another country. If we don't change our laws in Canada to deal with surveillance capitalism, is our democracy at risk?

Mr. Jim Balsillie: Without a doubt.

The Chair: Thank you.

Thank you all for appearing today.

The meeting is adjourned.