



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 123 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 30, 2018

—
Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 30, 2018

• (1100)

[English]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Good morning, everyone.

This is the Standing Committee on Access to Information, Privacy and Ethics, meeting 123. Pursuant to Standing Order 108(3)(h)(vii), this is the study of the breach of personal information involving Cambridge Analytica and Facebook.

Today we have with us from the Conservative Party of Canada, Trevor Bailey, the privacy officer and director of membership; from the Liberal Party of Canada, Michael Fenrick, constitutional and legal adviser, national board of directors; and from the New Democratic Party, Jesse Calvert, director of operations.

We'll start off with Mr. Bailey for 10 minutes.

Mr. Trevor Bailey (Privacy Officer and Director of Membership, Conservative Party of Canada): Thank you very much.

My name is Trevor Bailey. I'm the Conservative Party of Canada's privacy officer. I'd like to thank the committee for inviting me here today to discuss our privacy policy, and I look forward to answering any questions you may have surrounding that policy.

I've been the privacy officer for the Conservative Party for approximately one year in addition to my role as director of membership for the party.

The Conservative Party of Canada has had a formal privacy policy in place, including the role of privacy officer, for approximately six years. Though I am relatively new to this privacy role, I've held senior positions in the membership and fundraising departments for the past seven years. In those roles, I've had or shared the responsibility to oversee our data, access thereto and its authorized distribution.

The privacy officer role is built around our party's commitment to protecting the privacy of Canadians. This commitment is important to the Conservative Party of Canada. That commitment includes taking great care to keep both confidential and secure all information in our possession that relates to the personal information Canadians willingly provide to us or is passed to us by Elections Canada as laid out in the Canada Elections Act. That information includes surname, given names, civic address and mailing address. Other information the party may ask for and receive from individuals, like an email address, phone number, gender and date of birth, is also information

we include as covered by our privacy policy and is collected through our website or in response to a mail piece with that person's consent.

As part of our privacy policy, any person may unsubscribe from our email, mail or phone lists at any time using links provided in each email message, clicking on our privacy policy at conservative.ca or contacting the party directly.

As this committee would know, as a federal political party registered under the Canada Elections Act, the Conservative Party, including its electoral district associations, candidates, nomination contestants and leadership contestants, are subject to extensive regulation under that act, including in particular the public disclosure requirements for contributions over \$200. As a result of these requirements, we collect personal information from donors and members when they contribute to our party or purchase a membership. You may also choose to provide us with personal information on a voluntary basis such as when registering for an event or signing a petition. We are required by law to keep records of donors for tax purposes.

The information the Conservative Party gathers, either directly from Canadians or as a result of legislative requirements, is used for communication purposes. As a political party, we believe it is very important to communicate with Canadians on a regular basis. We are a national organization, but we have a riding-based membership system, so personal information may be disclosed to local riding associations, candidates, nomination contestants or leadership candidates for the purposes of communicating with those persons.

There is some non-personal information that we track that is also included in our privacy policy for the additional information of Canadians. That non-personal information that may be collected through our website is collected through the use of web cookies with the purpose of informing the party about how people use our website in order to help us deliver better content for those users or to assist in general advertising efforts. We inform people in our policy about how to opt out of many of the advertising features used by sites like ours by adjusting their Google Ads settings or through free services like the Network Advertising Initiative's consumer opt-out page.

To wrap up, the Conservative Party employs a variety of security systems to safeguard personal information from unauthorized access, disclosure or misuse, and from loss or unauthorized alteration. The Conservative Party does not and will not sell personal information.

As I said in the opening, the commitment to protecting Canadians' privacy is important to us, and ensuring it's kept safe and secure is something we take great care in doing.

If there are any questions on this policy, I'd be happy to take them.

Thank you.

• (1105)

The Chair: Thank you, Mr. Bailey.

Next up is Mr. Fenrick for 10 minutes.

Mr. Michael Fenrick (Constitutional and Legal Adviser, National Board of Directors, Liberal Party of Canada): Thank you.

Honourable members of the committee and Mr. Chair, it is a privilege to be able to speak with you today. I want to thank you for the opportunity for the Liberal Party of Canada to be heard on these important issues.

My name is Michael Fenrick, and as I was introduced before, I serve as the legal and constitutional adviser to the national board of directors. That's a volunteer position. I'm also a riding chair for the riding in my home community of Parkdale—High Park, so I also have the experience of working for the party and volunteering for the party at a local level.

Both from serving on our party's board and from working closely with grassroots volunteers, I know the party takes the protection of personal information extremely seriously. I also know how the responsible use of data can significantly increase participation and engagement in our political process.

Today, I hope to speak to you about both of those priorities, and I look forward to answering your questions.

First, I want to outline our most fundamental commitment on these matters. The Liberal Party of Canada works very hard both during and between elections to engage as many Canadians as possible in our democratic process. Protecting their personal information is a priority for the party in all of its interactions and operations.

As part of that commitment, the Liberal Party of Canada has a clear and strict privacy policy in place, which is posted on all of the party's national websites, and it can always be publicly viewed at liberal.ca/privacy. The highest level of security is implemented for all data and records that are maintained by the party. The party does not sell any personal information. At all times the Liberal Party of Canada fully complies with all Elections Canada rules and regulations for political engagement and campaign activities as required by our campaign partners, who do the same.

Why does all of this matter? Because secure and accurate data is very important to how modern political parties operate and engage with Canadians. Like all Canadian political parties, the Liberal Party uses data to engage with voters. Understanding the interests and the

priorities of Canadians helps us to speak to the issues that matter most to them and in turn mobilizes democratic participation in our country.

The importance of this objective truly can't be overstated. Political parties are not commercial businesses. We are not-for-profit voluntary associations defined in the Canada Elections Act as organizations whose fundamental purpose is to participate in public affairs by endorsing candidates for election. Our interests are very different from those of private sector entities to which federal privacy legislation applies. We promote candidates to Canadians. We're informed in part by information about eligible voters and in accordance with accepted privacy practices and safeguards, and we safeguard the information that Canadians entrust us with.

• (1110)

Using data to help engage voters isn't a bad thing; it's quite the opposite. It helps to ensure that political parties are in tune with what matters to the electorate and that more of us are involved in elections. For as long as there have been free and democratic elections, successful candidates have worked to build detailed lists of their supporters, to understand their priorities and return to them with an ask to help out at the polls.

Knowing what interests have motivated voters and who supports our party helps us deliver relevant information and policy positions to Canadians. For example, we know that more and more people, and especially young people, are seeking out news and information online. For parties to be relevant, we need to have a strong online presence and interact with Canadians through the mediums and on the platforms they are using. That's why in recent years innovative engagement on social media, online advertising and email communications has become increasingly important to our operations.

Where do we get the information we have about voters? Like the other registered political parties, we receive an electronic copy of the list of electors from Elections Canada each year. Under the Canada Elections Act, registered parties are authorized to use the lists to communicate with electors, including for the purposes of soliciting contributions and recruiting party members, in our case registered Liberals.

For all parties, using personal information contained in the list of electors in an unauthorized manner is a criminal offence under the act. It is punishable by a fine and up to two years of imprisonment. We take our obligations in this regard very seriously.

In addition, we work hard to identify, engage and mobilize potential supporters with phone calls, outreach events, door knocking, digital advertising, emails, petitions and more. Often we keep track of information about the issues that matter most to our supporters and to Canadians, and the information they express about whether they intend to vote for us. This information is recorded if it is volunteered by the individual voter and is used to inform the party's outreach efforts and political strategies at election time.

On occasion, limited types of data are purchased by the party to help us reach out and connect with more supporters and Canadians. For example, in the past we have purchased widely available phone book-type information or Canada Post address validation lists.

While we use social media to boost voter turnout, identify supporters through issues-based petitions and ask for fundraising support, the Liberal Party of Canada does not have access to specific Facebook accounts beyond those of our own social media channels.

Our party's primary voter-contact database is a system called Liberalist. Certain individuals, including MPs, riding association executives, candidates and campaign managers may request access to Liberalist. They can view the voter information for electors in their ridings.

Account holders are assigned certain levels of access based on our internal rules and policy, and must provide their name, email address, phone numbers, riding name and address. All account holders on Liberalist must agree to be bound by a Liberalist user agreement, which sets out the terms and conditions for using the system. A copy of that, I understand, is with the clerk.

• (1115)

Users must only use the data for the purpose of communication on behalf of the party with voters, donors and registered Liberals. They agree that they will not keep a copy of any of the data and will not share it with anyone else.

The Chair: Mr. Fenrick, you're about 15 seconds over. Are you just about at your conclusion?

Mr. Michael Fenrick: Yes.

I will take one moment to wrap up.

The Liberal Party of Canada also has a strict privacy policy in place. A copy has also been filed with the clerk of this committee. We think it is a best-in-class privacy policy for protecting the personal information of Canadians.

We hope this committee will seriously entertain submissions of the Liberal Party of Canada about the importance of political engagement as a guiding factor when considering these important issues.

Thank you.

The Chair: Thank you, Mr. Fenrick.

Next up, from the New Democratic Party, we have Jesse Calvert.

Go ahead, for 10 minutes.

Mr. Jesse Calvert (Director of Operations, New Democratic Party): Hello and good morning, members of the committee. My name is Jesse Calvert and I'm the director of operations for Canada's

New Democratic Party. I want to thank you for the invitation to appear before you to discuss our work with data and our privacy policies.

The federal NDP and most of its provincial sections across the country all use software called Populus to interface with our respective databases of elector data, similar in principle to both the Conservative Party's constituent information management system and the Liberal Party's Liberalist. Of course, the NDP has a unique structure, wherein the federal party and the provincial sections share a formal affiliation with a common membership.

While both the federal party and the provincial sections use Populus as a way to interface with their databases, the databases themselves are not shared. Information about electors is retained by the section collecting the data and each section uses the voters list from their respective elections agency, which is the permanent voters list produced by Elections Canada in our case, as the backbone of their own database.

With regard to membership lists, this information is handled by a single point of contact at the federal party and counterparts in the provincial sections. Each instance of Populus is separate from each other.

Populus is a web application developed by a third party contractor. This same company also developed foreAction, which is used by NDP caucus members and staff to track constituent case work. These programs are totally separate. They do not speak to each other and party staff, like myself, have no access to the case work database.

In terms of the data that we collect, like other parties, we use the Elections Canada permanent voters list, our own membership and donation lists, contact information from petitions, public data, such as from the census, and data collected as a result of direct outreach operations. We only use this data in accordance with our needs as a registered political party, and we do not give it to third parties, as a matter of policy.

We do not use any kind of psychographic modelling. Any modelling or analytics we do is based on publicly available statistical information and not personal private information. Nothing we use for these kinds of analytical purposes is more specific than, say, polling data or census information.

We understand that privacy is a serious concern and we strive to abide by the principles of PIPEDA. We have a designated privacy officer at the federal NDP, and recently put into place an updated privacy policy, which can be viewed at NDP.ca/privacy.

Here are some examples of how the party protects Canadians' privacy.

Every user of Populus must agree to terms of use before they are able to access the NDP database. Internally, we have secure protocols that govern who can access our data, what they can access and when they can access it. We abide by a principle of minimal access and only give users access to data that is relevant to their needs. For example, organizers in a given riding only have access to data in that riding. We offer electors the option to unsubscribe in every communication we have with them and we have internal security protocols to ensure that, in the event of a data breach, subjects are notified promptly.

We are in the process of moving our data into the cloud using the same provider that the Communications Security Establishment uses for unclassified data. One gap between our practice and PIPEDA that is currently in place is that we are unable to provide Canadians with their data upon request and give them the ability to correct it. This is mostly due to a lack of a security protocol to verify the identity of individuals requesting their data. We are giving this problem a lot of thought to determine how to address it properly.

● (1120)

In solving one problem, we do not wish to create another one. It's for that reason that we support a legislative change that would give Canadians the right to request their data and to extend the PIPEDA coverage to political parties, as is already the case in British Columbia through their legislation, PIPA. We need a consistent set of clear rules on privacy and personal data that all parties can abide by.

Thank you again for the invitation. I look forward to your questions.

The Chair: Thank you, Mr. Calvert.

We'll start off with Mr. Saini for seven minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much to all three of you for being here this morning. I'm going to start off with a general question first.

What protections are in place to keep the data you hold on Canadians safe? We can start with Mr. Bailey, and go that way.

Mr. Trevor Bailey: Certainly. Thank you, Mr. Chair.

There are really two elements to protecting the data. There is protecting against unauthorized access. We're talking about data breaches and attacks on our systems. That's obviously a continuing effort for us. We have a great team on that. That's not my expertise, but I do know that we have a very good data team in place. We test our systems constantly. We host in a very secure manner. We try to secure against any and all attacks. That's one side—the unauthorized access.

The other side, of course, is authorized access but inappropriate use. That would be where someone who has access in a limited capacity to the database would access information and use it in a way they were not authorized to do. We have significant policies and processes in place to minimize the impact or the opportunity for someone to do such a thing.

First and foremost is obviously limiting access to that data, so that, as my colleagues have mentioned, only people who have a need to access it have the opportunity to do so. Any of the information they do access is logged, and they are required to provide the reason for

this access. If and when it's used in an inappropriate manner, we have methods, both internally and, if necessary, with the relevant authorities to.... We would co-operate fully with any investigation if there were any breach of our privacy policy or, of course, any loss.

There are two elements to it. As far as protecting our data, we have a great IT team for that. Our data security is a continuing matter. I was just talking this morning about some of the firewall protections that we're updating. The other side, which is where people have the key but want to use it in an inappropriate manner, is primarily where our policies come into play. Certainly, the procedure is that we limit the breadth of access to data that any one user can have at one time.

● (1125)

Mr. Michael Fenrick: For our part, many of the same things that Mr. Bailey has spoken to apply equally with respect to the Liberal Party and its treatment of personal information. From the perspective of somebody outside the system gaining access, we regularly run training. We've developed a cybersecurity policy, and we regularly run training at all levels of the organization, in terms of trying to ensure that people are educated about how to avoid things like phishing scams, spoof email addresses and matters along those lines.

In addition to that, the Liberal Party's national director and the team at the head office here in Ottawa have met with the CSE in order to discuss best practices on how to secure Canadians' information. That includes using cloud-based email servers, which is what is recommended by the CSE. That has been implemented.

On the access by users who have been granted access, who are volunteers, there are a number of ways in which we protect that information. Probably the most important, though, is that it's a segmented database. You're only given access to the information on Liberalist that you need. That can be as little as a single poll or, in the case of somebody who is running a canvass, in fact, it could just be the canvass information for a particular block or two of a neighbourhood. Riding association presidents may have access to the entire riding. Very few people within the Liberal Party have access to the entire list of electors. Our database is segmented in order to ensure that only the access that you've been granted and that you need is given to you.

Mr. Jesse Calvert: Unsurprisingly, much of what my colleagues have just said applies also to the New Democratic Party. We have a varying degrees of access protocol to ensure that folks who have access to the database only have access to the information that they require to do their tasks, and only a very small number of IT professionals have full access to the information.

We also have a terms of use policy that all users are required to read and understand and consent to before they are given access to their particular segment of the database. Also, as I mentioned in my opening statement, we are in the process of moving our database and our systems into the cloud, which will increase our ability to secure the information that is contained within it.

In terms of guarding against security breaches, we have a number of internal security protocols that are constantly under review and being developed and improved upon. We have ongoing threat monitoring to ensure that if a breach were to take place, we would be able to respond quickly, swiftly. We have protocols for notification, if such a situation were ever to arise to ensure that the folks whose information might have been compromised are informed of that situation.

Mr. Raj Saini: This is my last question. Obviously you can appreciate there is a difference between a political organization and a private sector organization, and the collection of data that each one uses for its own purpose. In one regard, you're talking about a political entity that is using the data in the pursuit of democracy, and in the other, in a private sector organization, you're using that in the pursuit of profit.

Do you think the rules should remain the same or be subject to the same standards, or should there be a difference between political parties and private sector organizations?

• (1130)

Mr. Trevor Bailey: I could start off on that one.

You're absolutely right. They are separate. They are different. We currently operate under a different legislative situation, with PIPEDA coverage for private companies and not covering us as political parties.

My role with the party is to enforce our privacy policy as written, and currently it does not come up to full PIPEDA compliance, which I believe might be the suggestion there. We certainly cover all our legal requirements and we follow everything as laid out in the privacy policy, but the decision as to whether or not we should implement or change the legislative background that covers us as political parties, I leave to Parliament and to you, as a committee. We're here to enforce the rules as written, and if there's a new rule basis that comes in and takes effect for how we need to operate, then we would certainly come into compliance.

I don't have an opinion as to whether it would be required or not.

The Chair: Thank you, Mr. Bailey, and Mr. Saini.

Next up, for seven minutes, we have Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you very much, Chair. My apologies for my tardy arrival.

Thanks to all of you for coming today. It is much appreciated, and there is a very important discussion that we can have here today.

In June, after four months of study of what began as the Cambridge Analytica-Facebook-AggregateIQ scandal, the committee, among a number of recommendations to government in our interim report, recommended that political activities come under the

authority of the Privacy Commissioner of Canada. Mr. Calvert, you've already spoken to that.

As Mr. Saini pointed out indirectly, an awful lot of the testimony that we heard with regard to the Brexit referendum and interference, or attempted interference in the American political elections at different levels had to do with third party intervention. I'm wondering if each of you could comment—and Mr. Calvert a little more explicitly—as to whether or not each of your parties believes that extending the authority of the Privacy Commissioner to protect Canadians' privacy in the political sphere, as they are protected in the commercial sphere, would raise any objections with your respective parties.

We'll have Mr. Bailey first.

Mr. Trevor Bailey: Once again, as you mentioned, there was a lot of concern around third parties and their involvement. We certainly share that concern, and we want to make sure we have fair elections in this country, obviously. We play a large part in that, and we want to continue to be able to participate in the democratic process as fully as we possibly can.

That being said, as for whether there should be oversight by the Privacy Commissioner or enforcement of PIPEDA across political parties, once again I would leave that to Parliament to make that decision. My role as director of membership and privacy officer is to protect our lists, to make sure we take good care of them and to make sure everyone is treated fairly and evenly.

If anything above and beyond that came from Parliament, we would certainly come into compliance. As for whether we should, once again, I would leave that up to Parliament.

Mr. Michael Fenrick: From the Liberal Party of Canada's perspective, obviously it's a critical issue that we need to address in terms of third parties. I've already outlined some of the ways in which we are trying to both address those issues and constantly improve on them within the Liberal Party.

On the issue, more broadly, of PIPEDA's application to political parties, I think we would hope that one of the serious considerations that this committee would take under advisement is the fundamental difference—I would say, founded in the Charter of Rights and Freedoms—between political participation or engagement and commercial activity. Our courts have recognized that in a number of places, including in protection of freedom of speech, etc.

If we are going to develop rules, we need to develop rules that work for all people who participate in the political process in this country. I say that from the perspective of a party that had approximately 80,000 volunteers, I think, in the last election. We need rules that work for the volunteer who's an 18-year-old, just got interested in politics, belongs to a campus club and is signing up his friends, all the way to more sophisticated people who have worked on a variety of campaigns.

From our perspective, whatever rules are developed need to recognize that fundamental reality, that political parties are voluntary associations of volunteers, fundamentally, and that there are hundreds, if not thousands, of volunteers to every paid staff member. It would be a real disincentive to participation in the political process if people could face the kinds of penalties that exist for corporations, for instance, for non-compliance under PIPEDA. It would actually have a chilling effect, I believe, on our political process to do so.

• (1135)

Mr. Jesse Calvert: The New Democratic Party seriously believes that Canadians deserve to have trust in their democracy and to have trust in their political parties. We think that the only way to increase this trust and to increase transparency is to ensure that, first, all political parties are playing by the same rules, and second, there is the ability for oversight into the way the internal policies of the party are applied. It's for that reason that we have been calling, again and again, for the inclusion of political parties within the PIPEDA framework.

I do agree that there are differences between the way political parties do their work and the way other types of organizations do their work, and certainly there should be thought and consultation when moving toward a framework, but we are very clear. We do think parties should be included in PIPEDA. We do hope the government moves toward that goal. We believe that will increase the trust Canadians can have in the security of their information and their trust in their democratic process.

Hon. Peter Kent: Thank you.

Each of you has said that your party does not sell or distribute political data beyond the party. I ask each of you to simply acknowledge whether your party buys data from data brokers.

Mr. Trevor Bailey: I'll start off once again. Thank you.

We have a very similar process to that laid out by my colleague Mr. Fenrick. We receive our data from four main sources. We're very up front about all of these.

The primary one we don't purchase. It's provided to us as part of the electors list from Elections Canada. That is 90% of our data. It is the information about who is an eligible voter. That makes up the lion's share of what we have in our system.

We do purchase data from two sources. One is InfoCanada. It's basically the white pages. We buy the phone book, so we get some phone numbers to match up with those constituents who we get from the list of electors. The second one we purchase from is Canada Post's change of address list, so that our lists are as up-to-date as possible, because that is issued more frequently than the list of electors. We try to reconcile those two. That is it. We don't purchase from any other source.

The fourth source of data, I think we should make clear, is that which is provided voluntarily, primarily by our supporters, but sometimes by our non-supporters, when they make a contribution, show up at an event, purchase a membership, or if they were to contact us and indicate their support one way or another, or answer a phone call, survey or something of that nature. The only place we purchase data, to be very clear, is InfoCanada, which is the white pages, and—

The Chair: We're out of time, but Mr. Fenrick and Mr. Calvert, would you like to follow through with a quick answer?

Mr. Michael Fenrick: The Liberal Party of Canada is very consistent with what my friend from the Conservative Party just said. Mainly things like phone book information and Canada Post information are examples. Much of this, for instance, Canada Post information, is purchased in large part in order to validate donors and ensure that we are compliant with our obligations under the elections act when we're accepting donations. There are a lot of reasons that we buy. It's not just to communicate, but that is an important part of it, obviously.

The Chair: Mr. Calvert, quickly...

Mr. Jesse Calvert: I think generally the same would be said for the New Democratic Party. We also want to ensure that the data we have with respect to address and mailing information is as up-to-date as possible, and we purchase information from Canada Post to make sure that's the case.

• (1140)

The Chair: Thank you.

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

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Mr. Chair.

Thank you, gentlemen, for coming. On behalf of the New Democratic Party, with my colleagues here, I ask that you don't target us individually for dragging your parties' representatives into the light of day. We're just doing our job here.

Mr. Fenrick, in 2012-13, leading up to the 2015 election, it was common wisdom, heard on the radio and media, that the Conservatives were really good at micro-targeting. New Democrats weren't so bad at it, but we were really trying to pick up our game. Liberals didn't really micro-target. They did one-inch wide advertising across the country. It was seen that this would be a problem for the Liberals in 2015. Then the election came, and you guys stomped us. Your micro-targeting was really good.

How did that transformation happen? Who oversaw the creation of a very impressive Liberal data machine for 2015?

Mr. Michael Fenrick: That's not something I can speak to directly, but I would be happy to give whatever information I can to the committee at a—

Mr. Charlie Angus: That's our leader calling. He didn't like that question.

Voices: Oh, oh!

Mr. Charlie Angus: He wants me to ask it again. Sorry.

Mr. Michael Fenrick: My answer, Mr. Angus, is simply that I don't have that information available to me right now, but I'd be happy to identify that information for you at a future point.

Mr. Charlie Angus: Okay.

For the next election, it appears that your party will be working with Tom Pitfield and Data Sciences. He did work on the 2015.... What will the relationship be between Data Sciences and the Liberal Party, in terms of a digital strategy?

Mr. Michael Fenrick: I can speak generally. In terms of our involvement with any third party provider, we ensure that those third party providers are bound by privacy obligations similar to the ones we impose upon ourselves. We include, in agreements with third party providers, that their use of the data is similarly restricted in order to protect the privacy interests of the data holder or the personal information of those individuals.

Mr. Charlie Angus: Mr. Pitfield was pretty impressive in 2015. Is that why you're working with Data Sciences? Is it because of their expertise in doing this kind of electoral data running?

Mr. Michael Fenrick: I don't think I'm the appropriate person to answer that question.

Mr. Charlie Angus: Okay.

Mr. Bailey, one of the things we talked about this morning was protocols and limits to accessing databases. In 2011, when we had the Pierre Poutine scandal, apparently a young staffer was able to make calls based on the Conservative CIMS database.

How was it possible that someone, a young volunteer, was able to have access to the databases if we have protocols in place to limit access so that abuse doesn't happen?

Mr. Trevor Bailey: In 2011, the situation as described was in one riding. It was in the riding of Guelph. The young individual you identified was a member of the campaign in Guelph. He was a member of that team and thus did have access to the database for the region for which he was responsible, which was Guelph. The use of that data, particularly drawing non-supporter information with the purpose of deceiving those voters, was certainly a breach of privacy policy both then and now, as well as of Elections Canada law and significant laws.

We certainly were not pleased with that, and that is one of the reasons we now have a league-leading privacy policy. We have changed not only the policy. It's not just putting words to it. The ability to access data has changed significantly since that time, and I'm very confident in the processes we now have in place. The system at the time limited his access to only the region for which he had responsibility. That was one of the key limits at the time, but his access was approved by the campaign at that time, which was one of the checks against access.

It was a breach of our policy and a breach of Elections Canada law. We have evolved as an organization because of it, not just with respect to our policies but certainly with our procedures and the ability to access data. It has changed since 2011.

• (1145)

Mr. Charlie Angus: Thank you.

Mr. Calvert, part of the reason we have undertaken this study is the Cambridge Analytica scandal. It's not just a question of political parties having data, but to be able to micro-target the issue of manipulating voters online.

The question that's come up time and time again involves data points that are collected by parties, the psychographic modelling. Does the New Democratic Party have an identified number of points of information it would like per potential voter to know whether they're in our universe? How do you target voters? Are you using psychographic modelling or statistical modelling to identify where potential voters or non-voters are?

Mr. Jesse Calvert: Like all parties, we're trying to talk to the people who are most likely to care about the issues we care about. We're trying to identify the groups of people who are most interested in the issues we stand up and fight for every day. We use publicly available data to do this, but the data and information we use is not personal information. It's not personally identifiable information. It's information that's publicly available and speaks to trends and groups of individuals.

In the end, the goal of a political party is to engage Canadians in conversations, to learn more about them by asking good questions and to improve upon our policies by listening to those answers. That's what we try to do on a day-to-day basis, whether through our online outreach or through our door-to-door outreach. That's our mindset going into it.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

Next up, for seven minutes, is Mr. Baylis.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Mr. Calvert, you said the NDP would be happy to be subject to PIPEDA laws.

Mr. Bailey, would the Conservative Party be happy to be subject to PIPEDA laws?

Mr. Trevor Bailey: Once again, I'll leave it up to Parliament and your committee to make a recommendation on that. My role with the party is to protect our lists and to follow our policies. I think we have a very good, leading privacy policy, but as for whether it should be in place, I leave that—

Mr. Frank Baylis: Mr. Fenrick, do you have a position on that?

Mr. Michael Fenrick: Certainly not as PIPEDA currently stands.... It just doesn't make sense in the particular context in which political activities are—

Mr. Frank Baylis: You feel that the penalties are too heavy. Do they compare to B.C.? In B.C., there hasn't been a great drop off—at least, I'm not aware of it—of volunteers because they are subject to the B.C. privacy laws. However, you think that PIPEDA laws are more strict than the B.C. laws. Is that your concern?

Mr. Michael Fenrick: I don't know the B.C. law in any sort of detail, but I do believe that the way that the penalties operate will be a disincentive to people's participating if PIPEDA were to be applied.

However, I think it's important to have the complete context before making that decision.

Mr. Frank Baylis: Okay, but the penalties are what you're saying might worry volunteers. That is what is bothering you about PIPEDA.

Mr. Michael Fenrick: Absolutely, and it's also just not well-tailored to the political context where you're dealing with a mostly volunteer organization.

Mr. Frank Baylis: Whether you're subject to PIPEDA or some other laws, let's say we're talking about the parameters of use. You have this database. For example, should you be able to commercialize a database? Do you have any thoughts on that?

You've collected a ton of data. People are making money all over the place.

I'll start with you, Mr. Calvert.

Mr. Jesse Calvert: I would say absolutely not.

Mr. Michael Fenrick: Absolutely not.

Mr. Trevor Bailey: I would say the same, yes. We have no—

Mr. Frank Baylis: How about this? I have charities and charities often swap data. They say, "We have this pool of donors, and if you tell us your pool of donors, we'll tell you our pool of donors." Now you're not making money from your database, but you have a very valuable database and someone else may have a valuable database, not your competitors but some other company. Should you be able to trade that data, giving them some of your data and getting some of their data so that, together, you've built a stronger database?

Mr. Jesse Calvert: I think that Canadians expect that the information that we receive from Elections Canada and gather through our outreach efforts will be protected and kept within our database, so I think that's probably not something that we would find effective, efficient or correct.

• (1150)

Mr. Frank Baylis: You should not be allowed to share it, not for commercial benefit and not even for sharing to gather other data, like swapping data.

Mr. Jesse Calvert: I think that raises some serious questions, and if put on the spot, I would say probably not.

Mr. Frank Baylis: Mr. Fenrick.

Mr. Michael Fenrick: I'm not sure that I have an answer for you other than the more general answer, which is that we don't do it. We certainly don't share our information.

Mr. Frank Baylis: You don't do it because you don't do it, but theoretically some fourth person from a fourth party could do it, and we're now trying to figure out the parameters of use.

Do you think we should allow you to do it or not?

Mr. Michael Fenrick: I'm not sure that I have a position on that, but I'd be happy to get back to you.

Mr. Frank Baylis: Okay.

Mr. Trevor Bailey: As covered by our privacy policy, we collect it for the purpose of electioneering, for running a campaign, for contacting them for the purposes of winning an election. What you're describing doesn't fit with our policy, so no.

Mr. Frank Baylis: It doesn't fit with your policy in what way?

Mr. Trevor Bailey: In that it would be using our data that we have collected for a purpose other than getting us votes in the next election.

Mr. Frank Baylis: Right now you're writing the rules for yourselves. I believe we should write the rules for you.

Mr. Trevor Bailey: Right.

Mr. Frank Baylis: I'm asking you the question in this light, and I'd like an answer now. Do you think we should allow you to do that, yes or no?

Mr. Trevor Bailey: As I said before, if that's your decision as a governing Parliament—

Mr. Frank Baylis: But you're also saying that the Conservative Party doesn't do that—

Mr. Trevor Bailey: Correct.

Mr. Frank Baylis: —and that you'd be comfortable with a law that doesn't allow you to share that data.

Mr. Trevor Bailey: That would be in line with our policy, so yes.

Mr. Frank Baylis: Okay.

Mr. Michael Fenrick: Mr. Baylis, I'd just like to interject with one more point. Of course, the list of electors that we receive is subject to the Canada Elections Act, and that's the primary point, I think, for all three parties in terms of the information that we collect. There are penalties, quite steep and serious penalties, for using that information right now.

Mr. Frank Baylis: That's the list of electors that you've collected. I understood that. However, then you've added stuff through your door knocking and through your phone calls—that this person likes pizza and that person likes hamburgers—that helps you to sell them your political views. That's the data that I'm talking about. You're saying that you'd be comfortable if we did not allow you to share the data that you're collecting.

Mr. Trevor Bailey: As I said, I think that's a good suggestion, and if it fits with our policy, yes.

Mr. Frank Baylis: Mr. Fenrick, do you have thoughts on that?

Mr. Michael Fenrick: I don't actually have a position on that right now.

Mr. Frank Baylis: Okay.

I want to follow up on what Mr. Angus was asking about: micro-targeting. Right now we might collect people's religious leanings, people's ethnicities, what languages they speak and things of that nature. Do you see a limit to how far we should allow political parties to go?

If we pick up, for example, that a person is part of a hate group or a person has some sorts of views that are not acceptable in general society, you might be able to use that view. We see this in politics, so it's not hypothetical. We see this and it's used to push them a certain way. That's part of what we found out in this study and in other places.

How should we have parameters of what we should and should not allow you to do and collect? Is there anything that we should not allow you to collect?

Mr. Jesse Calvert: The information we collect about individuals is the information that they give us, and that seems like a good place to start....

Mr. Frank Baylis: Okay, if someone says, "I hate this ethnic group", are you going to collect that data?

Mr. Jesse Calvert: By hearing it, we would have it. That's certainly not information that's—

Mr. Frank Baylis: The person who heard it heard it, but did you put it in your database as a data point?

Mr. Jesse Calvert: I don't think so. I don't think we would be interested in that.

Mr. Frank Baylis: Then you didn't collect it. I'm asking you whether we should put parameters around what you can and cannot collect.

Mr. Jesse Calvert: I actually haven't thought too much about that question. I think it's a good question. We might be able to get back to you on more specifics about how—

Mr. Frank Baylis: Does your code of conduct, code of ethics, have any limits on that?

Mr. Jesse Calvert: I'd have to look into it. I don't believe so.

The Chair: Thank you, Mr. Baylis.

Next up for five minutes we have Monsieur Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

I'd like to thank the witnesses for being here this morning.

I have no doubt as to the sincerity of your remarks today. From my 30 or so years in politics, I can tell you that, even though we are now living in the computer age, we've learned absolutely nothing. Forty years ago, I was working with people who were 50 and 60 years old at the time and who had been in the field for 40 years. When election time came around, there were lists of electors with people's phone numbers, and they were the right phone numbers. Back then, it was easy. Everyone had phone books and they were very thick. When we received the list of electors with people's names and addresses, we could look them up in the phone book. In many cases, a single household would have four, five or six voters, all with the same telephone number. That's no longer the case today.

Unfortunately, the number of land lines has dropped significantly every single year since I entered federal politics, and this will be my fifth election. Today, only 30% to 40% of people have land lines. All the rest of voters have cell phones. We don't have access to cell phone numbers, making it increasingly difficult to reach all voters. One riding can have 90,000 voters. We can knock on 10,000 doors, but let's not kid ourselves, we also have to spend time reaching out to people by phone.

Nowadays, we hear a lot about profiling. We assume people vote a certain way because they have certain views, but we can't just call them on the phone. We assume they think a certain way and we use social networks like Facebook to reach those people because we can't talk to them otherwise.

Do you think we should be allowed access to the cell phone numbers of people on the list of electors? It's fairly easy to get the phone numbers of people with land lines, but we can't get cell phone numbers, and the issue is only going to get worse. Is that something we should ask for, as lawmakers?

My question is for all three of you.

• (1155)

[*English*]

The Chair: We'll start off with Mr. Calvert.

Mr. Jesse Calvert: I'm sorry, you're asking whether we think that political parties should be given cellphone numbers through, say, the permanent electors list that Elections Canada generates. Is that your question?

[*Translation*]

Mr. Jacques Gourde: Yes, that's what I was asking.

We can get people's land line numbers from online directories—since actual phone books have all but disappeared—but cell phone numbers are considered confidential and we don't have access to them. Not being able to communicate with voters is problematic in many ways, and it's getting worse every year. As people die, the proportion of land lines drops between 1% and 5% a year. Young people own only cell phones. In 15 years, just 20% of the population will be accessible to us by phone.

Should we raise the red flag to say that it's time to do something about this situation? It's a genuine problem, after all.

[English]

Mr. Jesse Calvert: Thank you for the clarification.

I think that society continues to change and technology continues to change, and the way we do things has to also continue to change. The goal of a political party, or at least our political party, the New Democratic Party, is to engage Canadians in meaningful conversations. Anything that, say, Elections Canada was able to provide to us to allow us to do a better job at that, we would generally be supportive of.

Mr. Michael Fenrick: On behalf of the Liberal Party of Canada as well, part of the reason that we were excited to have this opportunity today was to discuss how it is not just that we're going to protect Canadians' privacy, which is obviously of critical importance, but also how we are going to meaningfully engage Canadians in the 21st century in order to have those discussions. I'm not sure of the logistics around the particular cellphone issue, but I am aware of the statistics that you have cited to the committee here today.

I do think it's of concern that it is more difficult every year for political parties to actually have discussions, not just with their supporters but with all Canadians, in order to provide an opportunity to actually understand what the electorate is looking for, which is why I think all of the committee members are in this business.

The Chair: We're actually out of time so just a brief response, maybe 10 seconds or less, if you can.

Mr. Trevor Bailey: You described the situation very well.

It's more access to data for us that can be provided to us legislatively by Elections Canada. We put a lot of effort into acquiring that information, so if it can be provided to us we would welcome it.

• (1200)

The Chair: Thank you, Mr. Gourde.

Next up for five minutes is Mr. Picard.

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

First of all, the exercise you're doing will hopefully put trust back in our population, not just us. Our job is quite a victim of cynicism, but we need ways to make sure that people can trust our institution, if that's the exercise you're fulfilling.

My concern is about working with third parties. Do you sell your data to third parties?

Mr. Jesse Calvert: Absolutely not.

Mr. Michael Fenrick: Absolutely not.

Mr. Trevor Bailey: Absolutely not.

Mr. Michel Picard: Okay.

Do you rent your data to third parties?

Mr. Jesse Calvert: Absolutely not.

Mr. Michael Fenrick: Absolutely not.

Mr. Trevor Bailey: Absolutely not.

Mr. Michel Picard: Are you saying all the data we're working on in each of your respective organizations stays within the organization and any third parties that may want to access the data.... How do they proceed if they want to access your data? With research centres, academics and foundations that are supportive of your lines of policy, how do you manage dealing with third parties, then?

Mr. Trevor Bailey: We certainly are approached by third parties for that sort of thing from time to time. Our specific policy covers sharing, for our purposes, federally, as well as the local campaign level nominees. We recently had a leadership race and they were covered by that as well. Those are the only separate organizations—and of course they fall under the umbrella of the Conservative Party of Canada—that we share our information with.

Mr. Michael Fenrick: Other than sharing within the party itself with our provincial and territorial boards, not the provincial party, the Ontario Liberal Party, or what have you, but our provincial territorial boards, which are part of our national organization, and at the riding level, we don't share our information with anyone.

The only exception to that would be in circumstances where we have engaged a third party supplier. In those circumstances we ensure that there are contractual provisions in place in order to protect the use of that data. It's not selling it. It's not renting it. It's using it in order to engage Canadians through a phone bank, or what have you, in order to communicate with them.

Mr. Jesse Calvert: We also do not sell, rent or share our data with third party organizations. From time to time we contract with third party providers to do the work of the registered political party. We ensure that the contracts that we have with them include strict contractual obligations to protect the confidentiality of the information that they might have access to and that they agree to fall under any of the privacy provisions that folks working within the party also have to fall under.

Mr. Michel Picard: But the possibility remains that when we work with third parties as soon as they have their hands on data for the purpose of the agreement they have with you, we tend to lose control over what they do with the data, or is that...?

Mr. Jesse Calvert: At least for us the protocols in place when that happens are very strict.

If a third party contractor requires information of ours to do the job that we contracted them to do, they might have access on a read-only basis but they don't have the ability to, say, download the information, copy the information or take it off premises. Certainly, we think long and hard before we engage someone from the outside to help us with our work. Once we do make that decision, we ensure that strict policies are in place and that legal and contractual obligations are instituted before anything happens.

Mr. Michel Picard: By the way, in your presentation, you mentioned that you created your system or updated your system recently. What was the upgrade about? Was it about policies or data protection, and what triggered that?

Mr. Jesse Calvert: We are in the process of moving our IT systems to the cloud. We're moving away from the holding of information on the premises and moving it into the cloud. I'm not an IT professional, so I can't get into the specifics, but it's my understanding that, here in the 21st century, it is standard practice to increase security and increase a whole bunch of other operational abilities, one of them being the security of the data. That's the process that's ongoing right now.

• (1205)

Mr. Michel Picard: I feel generous. I'll leave you my last five seconds.

The Chair: Thank you.

You're next up for five minutes, Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

During the study of the Cambridge Analytica-Facebook-AggregateIQ scandal, we have heard repeated recommendations from academics, from IT experts and from social media security experts that, on the basis of what happened in the Brexit referendum, where confected third parties controlled and targeted advertising buys on social media—and the same thing in the United States—there was a common recommendation that a political registry of advertising buys be set up so that one could see transparently what ads were purchased by the political parties or by third parties and how they were targeted.

I wonder if each of you could comment on what your party position might be towards that sort of registry, to show how your advertising buys in the writ period or perhaps even the pre-writ period of a campaign would be applied.

Mr. Trevor Bailey: We can start on that, if that's all right.

Absolutely. We share the same concerns about third party involvement in the election—this past election and those upcoming. If there were to be some increased requirement for us to fully register all ad purchases across all channels so that they could be investigated on an individual level.... Of course, we are required to list all election expenses and we are currently complying with that requirement, but if what is required to clean up the election is to get to the individualized level, then I think that's something that we would be in favour of if it comes forward from Parliament.

Hon. Peter Kent: Mr. Fenrick.

Mr. Michael Fenrick: As well, obviously, Canadians have the right to expect an election that's not interfered with by third parties.

If that is a measure that goes some way towards addressing those concerns, then it would be one that certainly should be considered.

As I understand it—and I may be mistaken because I appreciate that all of you are much more expert in this issue than I am—if Bill C-76 is passed into law, it will contain some measures with respect to Facebook ads and other matters. Many of these issues may be addressed by that legislation, and we welcome that.

Mr. Jesse Calvert: I think that generally the New Democratic Party has and will continue to stand up for more open and more transparent elections. As I've said, we do think that a political party should be brought into the PIPEDA framework, and I think that any measure that increases transparency increases the confidence that Canadians have that political parties are all playing by the same rules.

Hon. Peter Kent: One of the loopholes that wasn't addressed or is not being addressed by Bill C-76 is the fact that charitable American dollars that might have a political objective in determining, supporting or affecting a Canadian election can be effectively converted into Canadian dollars by being transferred from that American charitable group to the Canadian charity, which can then distribute them to third parties to be used in election campaigns. The witness who most effectively made this point, Vivian Krause said that it's easy for any individual political party to say that they take the high road in a political campaign if a third party is throwing the mud and making the political accusations on the campaign trail.

I wonder if any of your parties would encourage the government to more effectively enable the CRA to respond to Elections Canada's unknowns about how these foreign charitable dollars are getting into the Canadian election process.

Mr. Trevor Bailey: I'll get started on that one, if that's okay.

There are a couple of things. Other than working with Elections Canada on Bill C-76 consultation and any ongoing consultation on this matter, that's a bit outside my purview as privacy officer and membership chair. I'm not sure I can speak for the party on that particular issue other than, obviously, we want to make sure we have fair elections going forward.

• (1210)

Mr. Michael Fenrick: That's outside my purview as well. However, I can say quite strongly that obviously the Liberal Party is concerned about foreign money and its potential influence on our election.

Other than that, I don't think I can comment on that specific legislative suggestion.

Mr. Jesse Calvert: New Democrats are certainly concerned about foreign influence, whether it be monetary or otherwise. As I've said again and again, transparency is good. We believe in transparency and we think it increases the confidence of all Canadians in the democratic process.

Without knowing the details of that specific recommendation, in general, transparency when it comes to elections is a good thing.

The Chair: Thank you, Mr. Kent and everybody.

Next up is Madame Fortier for five minutes.

[*Translation*]

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

This morning, I realized that I had been a party volunteer for 25 years. It's worth noting that 25 years ago, we weren't talking about these rules, policies or codes of conduct. We are talking about them today, though. Protecting Canadians' information and making sure protocols are in place is important. I'd like to ask a few questions about what's happening on the ground. I think political parties have put codes of conduct in place, but I'd like to know what's actually happening on the ground.

How can parties make sure volunteers know about these policies, for instance, within the Federal Liberal Riding Association of Ottawa-Vanier? Can you tell us how you make sure that the people working on the ground understand the importance of protecting Canadians' personal information?

Mr. Bailey, you can go first. Please keep your answer brief.

[*English*]

Mr. Trevor Bailey: Absolutely, that's a great question.

We take it very seriously that we train our local volunteers. You're right; there are several levels of volunteers that exist, by their level of involvement. Mr. Fenrick mentioned earlier that it would be very difficult to impose stiff penalties upon someone at a lower level, so that works in a couple of different ways. One is that you need to provide them training and only provide them access to what they should have access to.

Most of our volunteers don't have access to any data. They should know that we'd have privacy policies and that they are covered by them because they are an extension of us during that time, but we need to limit the access to only those who truly need it. That comes from training at the local level. It comes from training of campaign managers. It comes from properly vetting all access so that we can effectively start up a campaign quickly and be compliant with any and all regulations.

[*Translation*]

Mrs. Mona Fortier: Mr. Fenrick, would you like to answer the question?

[*English*]

Mr. Michael Fenrick: Training is huge and key at all levels of the volunteer chain, including at the very basic level where people are out canvassing and have information. Obviously, limiting access as well, so people only have access to the information they need is

important, and in addition to that, where people do have access, ensuring that there are protections in place.

We have our Liberalist user agreement, where anybody who has access to it is bound by it and has agreed to ensure to hold that information and to return it at the end of their use so that they actually don't maintain any of that information. They're reminded of those obligations from the very moment they begin to have any access to it.

[*Translation*]

Mrs. Mona Fortier: Mr. Calvert, would you like to answer as well?

[*English*]

Mr. Jesse Calvert: Training is top on the list, and continued reinforcement of the importance of not just reading but understanding the protocols that are in place when they're given access or given a piece of information. It's why, if you are granted access to a Populus instance, where you might have access to a segment of information, you actually have to log on and read through the terms of use and take an affirmative step by saying, yes, you agree to this, and clicking the button. We try to write those in the clearest possible terms. That's why we have a privacy officer, not just to hear complaints but also to be a point of contact for individuals throughout our organization to ask questions.

You're absolutely right. Things have continued to change over the last 25 years. Certainly my generation, the younger generation, is very aware of the new world we're living in, so it's important for us to provide a point of contact for people throughout the organization to ask the questions they have.

• (1215)

[*Translation*]

Mrs. Mona Fortier: I'm going to stay on the topic of privacy protection.

We talked about third parties. Specifically, how do your parties protect against the inadvertent or unauthorized disclosure of data to third parties, as far as volunteers and staff members go? How do you monitor that? How do you evaluate that?

[*English*]

Mr. Trevor Bailey: Once again, I'll jump in first.

Absolutely, sharing information with third parties is of significant concern. As I mentioned, the security of our data is split into the two methods: protecting the data, and protecting against unauthorized access. It is evolving, but we certainly have an organization and leading privacy policy, which I haven't mentioned explicitly, and they do sign those agreements.

We start anywhere from, as the first step, simply cutting off access and then investigating it, to issuing cease and desists both to the individuals who have drawn the information and anyone who we believe has access to it. In terms of legal involvement, our legal team will get involved quickly if we feel that it has been used.

It's requested, and in fact demanded, that they destroy any copies of data if it came from our source and was used inappropriately. Then, of course, with any type of authorities that we need to go to further, if there are other rules or laws that have been broken, particularly Elections Canada laws, which are pretty broad on this topic, we co-operate with any and all investigations. Our data is our most valuable asset.

Mrs. Mona Fortier: My time is up, but if ever you could share your information....

The Chair: Could we get brief answers from Mr. Calvert or Mr. Fenrick?

Mr. Michael Fenrick: Sorry, did I understand the question correctly? Is it about inadvertent disclosure? Is that the issue?

Mrs. Mona Fortier: Yes.

Mr. Michael Fenrick: The Liberal Party of Canada regularly does training with its staff in order to address issues along the lines of when you get spoof emails and phishing scams. We regularly get involved in those sorts of security processes to ensure that the information is not disclosed.

The second piece just comes back to the segmented database we use, which is not simply to provide limited scopes of access to users. The database itself is segmented such that it is a more secure way of proceeding, such that information can only be accessed in tranches, rather than the complete information.

The Chair: Mr. Calvert, it has to be a much quicker answer than that, if you can.

Mr. Jesse Calvert: We protect it through limiting access, ongoing threat monitoring and extensive training.

The Chair: Well done.

Mr. Cullen, you're last up. Welcome back. You have three minutes.

Mr. Nathan Cullen (Skeena—Bulkley Valley, NDP): Jesse, are you sure you're a New Democrat? That was awfully concise.

Let's try for concision in this little speed round.

Thank you for being here. It's fair to say that in order for your parties to be effective, you need to be able to communicate with voters, and in order to do that effectively, you need to understand voters at an individual level. Each party collects information on individual Canadians in terms of voting intention, where they live and voter ID. Is that correct?

Mr. Michael Fenrick: Correct.

Mr. Nathan Cullen: I was just establishing that.

That has increased over time, in terms of the wealth, depth and breadth of the information that each of the parties holds about individual Canadians. Is that also true? Compared to 20 or 30 years ago, is it fair to say that what we know about individual voters has increased significantly?

Mr. Trevor Bailey: In terms of quicker and more response time, online contacts....

Mr. Nathan Cullen: In terms of online contacts and social media, is that fair to say?

Mr. Michael Fenrick: Yes.

Mr. Nathan Cullen: Okay.

Last June, this committee passed a decision that the parties should fall under privacy laws, PIPEDA specifically. Do you support that recommendation?

I'll start with our Conservative friend.

Mr. Trevor Bailey: As I mentioned a couple of times earlier in this room, I would leave that to Parliament. As the party, we would enforce whatever rules are placed upon us to make sure we're compliant.

Mr. Nathan Cullen: Would you be able to enforce such a rule?

Mr. Trevor Bailey: It would require significant consultation and development or redesign of our processes, but—

Mr. Nathan Cullen: You could do it.

Mr. Trevor Bailey: —if it was brought into law, we would certainly continue to exist as a party.

Mr. Nathan Cullen: Mr. Fenrick.

Mr. Michael Fenrick: We would not support the application of PIPEDA en masse and en bloc to political parties in the sense that, as it's currently drafted, it's intended to address commercial activity. It's not intended to address political activity.

Mr. Nathan Cullen: Right now, we have no laws governing privacy in political parties. As it was described by the Privacy Commissioner, it's the wild west.

According to the Chief Electoral Officer, Bill C-76, which you referenced earlier, has nothing of substance in it when it comes to privacy. The status quo will continue, which is that none of you are under any legal obligations when it comes to privacy as pertains to the federal laws. Is that right?

Mr. Michael Fenrick: As it currently stands, there may be certain situations, but I don't think I can speak to that issue directly. What I can say is that PIPEDA, as it currently stands, is not an appropriate tool for managing political parties and political engagement in this country.

• (1220)

Mr. Nathan Cullen: That's interesting because we even recommended one step down from PIPEDA, and your representatives from your party rejected that as well. The status quo is nothing. The Chief Electoral Officer and the Privacy Commissioner have all recommended that we have something. What's the New Democrats' position on this?

Mr. Jesse Calvert: As I've said a number of times in this proceeding, we have said as a party before, and will continue to say, that we thoroughly believe that all political parties should be playing by the same rules. There should be a clear set of rules. We believe that the way to do that is to bring political parties under the jurisdiction of PIPEDA.

Mr. Nathan Cullen: You're all keen observers of politics. You watched the recent U.S. presidential election, the Brexit referendum that happened in England, the implications of Cambridge Analytica

The Chair: Three minutes go by very quickly, Mr. Cullen.

Mr. Nathan Cullen: Let me just end on this.

Twenty-three years ago today we had a referendum in this country in Quebec. If a similar referendum were held in these contexts right now and the political parties were hacked because there wasn't proper privacy protections in law, imagine the result of that vote in Quebec, as it was with Brexit in England. There would be suspicion and the reality of foreign influence over a referendum question. A pivotal referendum question in Canada would be affected by outside sources.

Would that real threat not present us with more urgency to actually do something about this in Canadian law, something that you, apparently, could abide by if we passed such legislation?

The Chair: That's a great question to leave hanging in the room as we close today.

Thank you for coming today, Mr. Bailey, Mr. Fenrick and Mr. Calvert. We much appreciate your attendance at our committee as the officially recognized parties. Again, thank you for your appearance today.

The meeting is adjourned.

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <http://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : <http://www.noscommunes.ca>