HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 118 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 2, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 2, 2018

● (1105)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Welcome this morning to the Standing Committee on Access to Information, Privacy and Ethics for meeting number 118. Pursuant to Standing Order 108(3)(h)(vii), we are continuing our study of breach of personal information involving Cambridge Analytica and Facebook.

Today we have as witnesses Elizabeth Dubois, Michael Pal and Samantha Bradshaw.

We'll start off with Ms. Dubois for 10 minutes.

Dr. Elizabeth Dubois (Assistant Professor, Department of Communication, University of Ottawa, As an Individual): Hello. Thank you for inviting me to speak today.

I am an assistant professor at the University of Ottawa. I completed my doctoral work at the University of Oxford. My research focuses on political communication in a digital media environment. I've examined issues such as the political uses of artificial intelligence and political bots, echo chambers, and citizens' perceptions of social media data use by third parties, such as government, journalists and political parties.

My research has been conducted in Canada and internationally, but today I want to speak about four things: first, analog versus digital voter-targeting strategies; second, changing definitions of political advertisements; third, self-regulation of platforms; and fourth, artificial intelligence.

I have one quick note. I'll use the term “platform” throughout my testimony today. When I do, I'm referring to technology platform companies, including social media, search engines and others.

Let's start with voter targeting. This is by no means a new phenomenon. It's evolving at a spectacular rate, though. It is typical and in fact considered quite useful for a political party to collect information by going door to door in a community and asking people if they plan to vote and who for. In some cases, they may also ask what issues a citizen cares about. This helps political parties learn how to direct their limited resources. It also helps citizens connect with their political system.

However, even with this analog approach, there are concerns, because disengagement of voters and discrimination can be exacerbated. For example, if certain groups are identified as unlikely voters, they are then essentially ignored for potentially the remainder of the campaign.

Digital data collection can amplify these issues and present new challenges. I see four key differences in the evolving digital context as opposed to that analog one I briefly outlined.

First, there are meaningful differences between digital and analog data. The speed and scope of data collection is immense. While data collection used to require a lot of human resources, it now can be done automatically through sophisticated tools. I believe that last week you heard from a number of people who described the ones that political parties are using currently.

Similarly, this data can now more easily be joined with other datasets, such as credit history or other personal information that citizens may not want political parties or political entities to be using. It can also be more easily shared and transported and more easily searched, and predictive analytics can be employed because there is so much more data and there are so many more kinds of data that they can be collected together and analyzed very quickly.

Second, citizens may no longer be aware when their data is being collected and used. Unlike when they had to answer the door to give out personal information, this now can be done without their knowledge. They may not even know what is technically possible. In a study of Canadian Internet users, my colleagues at Ryerson University and I found that most Canadians are uncomfortable with political uses of even publicly available social media data. For me, this signals a need to really think about what kinds of data citizens would actually want their political representatives to have and to be using.

Third, the uses of data are evolving. Since online advertisements, for example, can now target niche audiences, personal data has become more useful to political entities. At the same time, these uses are less transparent to regulators and less clear to citizens. This means that emerging uses could be breaking existing laws, but they're so hard to trace that we don't know. We need to have increased transparency and accountability in order to respond adequately.

Fourth, political entities are incentivized to collect data continually, not solely during an election campaign. This means that existing elections laws could be insufficient. I should note that it is not just political parties that are collecting this kind of data, but also non-profits, unions and other third parties, so the questions about how this data is collected and what is the responsible use have to be broader than simply political parties writ large.

These changes are particularly concerning, then, because many of these uses aren't covered by existing privacy laws, and the Privacy Commissioner doesn't have the tools needed to make sure those laws are enforced the way they were intended.

This data use is not all bad. There are a lot of positive uses, including increasing voter turnout and trying to combat voter apathy. That said, to balance things we need to make sure we include political parties under the personal data uses laws that we have, PIPEDA being the main one. We need to create provisions that ensure transparency and accountability for political uses of data, and we need to ensure that citizens are literate, which includes things like having better informed-consent statements and other media and digital literacy initiatives.

With the few minutes I have left, I want to talk about a few issues that stem from this targeted voter behaviour. First is political advertisement. It's no longer quite as clear-cut as it once was. In addition to the placement cost for what platforms might call advertisements, there are a bunch of other ways that political entities can have paid content show up in somebody's newsfeed or as a recommended video, and how algorithms can be gamed to make sure that certain pieces of content show up on people's screens.

Those might include something like sponsored stories, using brand ambassadors, renting social media accounts that already have a big following, or employing political bots to help disseminate information more widely. All of these could be done potentially for free but they could also be done on a paid basis, and when they're paid, that comes awfully close to advertising, under the spirit of the law.

In response, we need to redefine what constitutes a political advertisement in order to continue enforcing these existing laws and their intended outcomes. It's particularly important that we consider this when we look at the worldwide increase in instant messaging platform use. The ways that political parties and other political entities are using instant messaging platforms is a lot harder to track than the ways social media platforms are used, and we can expect that is going to increase.

Second, I want to talk about self-regulation and how it is insufficient when we're talking about the big platform companies. While they have been responding, these are reactionary responses. These are not proactive responses to the threat that we see when digital data is being collected and personal information is being stored. These companies need to be responsible for the content that shows up, what they allow to show up, on their platforms. We also need to make sure that any interactions they have with those data are transparent and accountable. Right now there is a black box. We don't know how Facebook or Google decides what shows up and what doesn't, and we can't allow that to continue when things like personal privacy, hate speech, and free speech are being called into question.

Finally, the use of artificial intelligence is already complicating matters. The typical narrative at the moment is that when learning algorithms are used, it is impossible to open that black box and unpack what's happened and why. While this may be true if you take a very narrow technical perspective, there are in fact steps we can take to make the use of AI more transparent and accountable.

For example, we could have clearer testing processes, where data is open for government and/or academics to double-check procedures. There could be regular audits of algorithms, the way financial audits are required, and documented histories of the algorithm development, including information about how decisions were made by the team and its members and why. We also need things like clearer labelling of automated accounts on social media or instant messaging applications, and registrations of automated digital approaches to voter contact. You could imagine a voter contact registry being modified to include digital automated approaches. As well, we need widespread digital literacy programs that really dig into how these digital platforms work so that citizens can be empowered to demand the protection they deserve.

Ultimately I see a lot of value in political uses of digital data, but those uses must be transparent and accountable in order to protect the privacy of Canadians and the integrity of Canadian democracy. This requires privacy laws to be updated and applied to political parties, the Privacy Commissioner to have increased power to enforce regulations, and platforms to be held responsible for the content they choose to allow and the reasons for that.

Thank you.

● (1110)

The Chair: Thank you, Ms. Dubois.

Next we have Michael Pal.

Professor Michael Pal (Associate Professor, Faculty of Law, Common Law Section, University of Ottawa, As an Individual): Thank you very much for having me today.

I'm an associate professor in the faculty of law at the University of Ottawa, where I teach election law and constitutional law. Also, I am the director of the public law group there, although today I speak only for myself. I work on matters including voter privacy, campaign finance laws applied online and social media platform regulation, in addition to election cybersecurity. Today I'd like to speak to you a little bit about political parties, which I know is something you've heard a lot about, about social media platform regulation, and then about cybersecurity, briefly, I think, given what you've heard in the last few rounds of testimony.

Some of this material I had the opportunity to present to your colleagues in the procedure and House affairs committee in their study of Bill C-76, so I also have a few comments about that bill.

The first issue, which I know you've heard about, is voter privacy as it relates to political parties. As my colleague Professor Dubois mentioned, political parties are one of the few major important Canadian institutions and entities not covered by meaningful privacy regulation. They are not government entities under the Privacy Act, and they are not engaging in commercial activity under PIPEDA. They fall into a gap between the two major pieces of federal privacy legislation.

Very recently, all of the privacy commissioners across Canada—the federal commissioner and the provincial ones—issued a statement saying this was an unsatisfactory state of affairs and something needed to be done about it. Only in B.C. are political parties covered by provincial privacy laws. There was a bill in Quebec, as I know you've heard, which was not passed before the recent election.

Bill C-76 would address these measures to some extent. Mainly, though, it would require political parties to have privacy policies and set rules on which particular issues the policies must address. All the major registered parties already do have privacy policies. The bill might change some of the issues that they address, because they're not consistent across all parties, but it would not actually clearly give oversight authority to either the federal Privacy Commissioner or Elections Canada. It would not actually require specific content in privacy policies. It wouldn't provide an enforcement mechanism. Therefore, I think, it's a good first step. It's the biggest step that's been made in terms of political parties and privacy, but it doesn't go far enough.

What would regulation of political parties to protect voter privacy look like? Voters should have the right to know what data political parties hold about them. Voters should have the right to correct incorrect information, which is pretty common under other privacy regimes. Voters should have comfort that political parties should only use the data they collect for actual legitimate political purposes. As Professor Dubois mentioned, it's a good thing that political parties collect information about voters—you can find out what voters actually want and you can learn more about them—but that data should only be used for political purposes, electoral purposes.

One place where I think some of the other generally applicable privacy rules would not work here is, say, on a “do not call” list. Political parties should be able to contact voters, and it would be a problem, I think, for democratic electoral integrity if 25%, 30% or 40% of voters were simply uncontactable by political parties. I think we have to actually adapt the content of the rules that are out there for the specific context of political parties and elections.

The second big issue I wanted to address is social media platform regulations. I know you've heard a lot about Facebook. A lot of this is contained in a paper I gave recently at MIT, which I'm happy to share with the committee if it's useful. The Canada Elections Act and related legislation governs political parties, leadership candidates, nomination contestants and third parties, as you well know. Social media platforms and technology companies need to be included under the set of groups that are explicitly regulated by electoral legislation and the legislation that is under the purview of this committee. How so? Platforms should be required to disclose and maintain records about the source of any entities seeking to advertise on them.

Bill C-76 does take some positive measures there. It would prevent, say, Facebook from accepting a foreign political advertisement for the purpose of influencing a Canadian election. That's a good step forward. It only applies during the election campaign, as I read it, and I would like to see a more robust rule that requires due diligence on the part of the social media companies. Is there a real person here? Where are they located? Are they trying to pay in rubles or dollars? Do they have an address and other basic things that we would all pretty logically think of doing, if you cared about the source of the donation.

● (1115)

That relates to foreign interference. It also relates to having a clean domestic campaign finance system, given all the advertising that happens online.

Another issue that I think requires further regulation is search terms. You can microtarget ads to particular users of a social media platform. If there's a political election ad on Hockey Night in Canada, we get to see the content of the ad. As members of the public, we don't necessarily get to see an ad that's microtargeted at an individual or a group of individuals and those individuals might not even know why they were targeted.

There are certain kinds of searches that we may think have no place in electoral policy. For instance, searching for racists is something you can do, potentially, and there's been a lot of media discussion about that and whether that did happen in the last U.S. election. I don't think we have concrete information about particular instances, but we know enough to know that search terms might be used in a way that we find objectionable, in broadly understood terms about how democracy should operate in Canada.

Therefore, there's a public value in disclosing search terms, but also to the individuals that have been targeted who may not know why.

Another issue is that there should be a public repository of all election-related ads. Facebook has voluntarily done some of this. That decision could be rescinded at any point by people sitting in California. That's not an acceptable state of affairs to me, so that should be legally mandated.

A very interesting precedent has been raised about political communication on WhatsApp. There's even less publicity about what is sent on text messaging, especially for encrypted end-to-end applications, like WhatsApp. It came out in the media recently that, in the Ontario provincial election, there were political communications on XBox. I don't use the XBox. I don't play a lot of video games, but people who do can be targeted and have election ads directed to them. In the public, we have no way of knowing what the content of those ads are, so public disclosure of election ads on an ongoing basis, not just during the election campaign, on all the relevant platforms is something that I would like to see.

Another matter is social media platforms and whether they should be treated as broadcasters. I'm not an expert in telecommunications law. I don't make any claims about whether, say, Facebook should count as a broadcaster, like CTV or CBC, generally. However, there are provisions in the Elections Act related to broadcasters, in particular section 348, which says that the broadcaster must charge the lowest available rate to a political party seeking to place an ad on its platform. This ensures that political parties have access to the broadcasting networks, but it also ensures that they're charged substantially the same rate. Therefore, CTV cannot say, “We like this party, so we're going to charge them less. We don't like that party, so we're going to charge them more”.

Facebook's ad auction algorithm potentially increases a lot of variation and the price that an advertiser might pay to reach the exact same audience. That is something that I think is unwelcome because it could actually tilt the scale in one direction or another.

We have a bit of a black box problem with the ad auction system. Facebook doesn't tell us exactly how it works because it's their proprietary information, but on the basis of the information we know, I think that there is something there for regulation under section 348, even if we don't treat Facebook like a broadcaster more generally.

The second last thing is liability. One way to incentivize compliance with existing laws is imposing liability on social media platforms. Generally, they're not liable for the content posted on them, so one of the big questions, before this committee and the House in general, is whether there should be liability for repeated violations of norms around elections. I think that's something that we may need to consider.

The last point I wanted to make is simply on election cybersecurity, because I understand that's something of interest to the committee. Cybersecurity costs a lot of money. For example, I think that Canadian banks spend a lot of money trying to ensure cybersecurity. It may be difficult for political parties or entities involved in the electoral sphere. Political parties receive indirect public subsidies through the rebate system, say, for election expenses. One way to incentivize spending on cybersecurity is to have a rebate for political parties or other entities to spend money on cybersecurity. That's an idea that I've been trying to speak about quite a bit lately.

● (1120)

The last issue is that the U.S. has come out with very detailed protocols on what should happen among government agencies in the event of a cyber-attack, an unfortunate potential event, say, in the middle of the October 2019 election. What would the protocols be? There may be discussions that I'm not privy to between Elections Canada or the new cybersecurity agency. I hope there are, but the public needs to have some confidence about what procedures are followed, because if they don't know what the procedures are, there can be risks that an agency is seen as favouring one side or another, of foreign interference, potentially, on behalf of one party or one set of entities. I think that's pretty self-evident based on what has happened in the U.S.

Some more publicity around those protocols, I think, would be very welcome.

Thank you very much for your attention. I look forward to your questions in either official language.

The Chair: Thank you, Mr. Pal.

Last up, via teleconference, we have Samantha Bradshaw.

Go ahead for 10 minutes.

Ms. Samantha Bradshaw (Researcher, As an Individual): Great.

Thanks for having me today.

My name is Samantha Bradshaw. I'm a researcher on the computational propaganda project at the University of Oxford. I'll shorten that to Comprop.

On the Comprop project, we study how algorithms, big data and automation affect various aspects of public life. Questions around fake news, misinformation, targeted political advertisements, foreign influence operations, filter bubbles, echo chambers, all these big questions that we're struggling with right now with social media and democracy, are things that we are researching and trying to advance some kind of public understanding and debate around.

Today I'm going to spend my 10 minutes talking through some of the relevant research that I think will help inform some of the decisions the committee would like to make in the future.

One of our big research streams has to do with monitoring elections and the kinds of information that people are sharing in the lead-up to a vote, and we tend to evaluate the spread of what we call “junk news”. This is not just fake news and not just information that is false or misleading, but it also includes a lot of that highly polarizing content—the hate speech, the racism, the sexism—this highly partisan commentary that's masked as news. These are the kinds of junk information that we track during elections. In the United States, that was one of our most dramatic examples of the spread of junk news around elections. We found about a 1:1 ratio of junk information being shared to professionally produced news and information.

What's really interesting here is that if you look at the breakdown of where this information was spreading most, you see it tended to be targeted to swing states, and to the constituencies where 10 or 15 votes could tilt the scale of the election. This is really important because content doesn't just organically spread, but it can also be very targeted, and there can be organized campaigns around influencing the voters whose votes can turn an election.

The second piece of research that I'd like to highlight for everyone here today has to do with our work on what we call “cyber troops”. These are the organized public opinion manipulation campaigns. These are the people who work for government agencies, political parties or private entities. They have a salary, benefits. They sit in an air-conditioned room, and it's part of their job to work on these influence operations. Every year for the last two years we've done a big global inventory to start estimating some of the capacities of various governments and political party actors in carrying out these manipulation campaigns on social media.

There are a few interesting findings here. I'm not going to talk about all of them, for sake of time, but I'd like to highlight what we're seeing in democracies and what some of the key threats are. For democracies, it tends to be the political parties who are using these technologies, such as political bots, to amplify certain messages over others and maybe even spreading misinformation themselves in some of the cases we've seen. They tend to be the ones who use these organized manipulation tactics within their own population.

We also tend to see democracies using these techniques as part of more military psychological or influence operation activities. For the most part, it's the political parties who tend to focus domestically. We also see a lot of private actors being involved in these sorts of campaigns around elections, so where a lot of the techniques around social media manipulation were developed in more military settings for these information warfare techniques back in 2009 or 2010, now it tends to be private companies or firms that are offering these as services. Companies such as Cambridge Analytica are the biggest example, but there are so many different companies out there who are working with politicians or with governments to shape public discussions online in ways that we might not consider healthy for democracy and for democratic debate.

● (1125)

I guess the big challenge for me when I'm looking at these problems is that a lot of the data that goes into the targeting is no longer being held by the government, by Statistics Canada, which is the best information about Canadian public life. Instead it's being held by private companies such as Facebook or Google that collect personal information and then use that to target voters around elections.

In the past, it was all about targeting us commercially to sell us shampoo or other kinds of products. We knew it was happening and we were somewhat okay with it, but now when it comes to politics, selling us political ideologies and selling us world leaders, I think we need to take a step back to critically ask to what extent we should be targeted as voters.

I know that a lot of the laws right now are around transparency and improving why we're seeing certain messages, but I would take that a step further to ask if I should even be allowed to be targeted because I'm a liberal or on a even more microscale than that.

I know one of my colleagues earlier talked about targeting because you are identified as being a racist. At those much deeper levels as to who we are as individuals that really get to the core of our identity, I think we need to have a serious debate about that within society.

In terms of some of the future threats we're seeing around social media manipulation, disinformation and targeted advertisements, there are big questions around deep fakes and artificial intelligence making political bots a lot more conversational so that the person behind the account or the bot behind the account is human and more genuine. That might make it harder for citizens and also the platforms to detect these fake accounts that are spreading disinformation around election periods. That's one of the future threats on the horizon.

Professor Dubois talked about messaging platforms, things like WhatsApp and Telegram. A lot of these encrypted channels are incredibly hard to study because they are encrypted. Of course, encryption is incredibly important, and there's a lot of value in having these kinds of communication platforms, but the way they are affecting democracy by spreading junk information raises serious questions that we need to tackle, especially when you look at places like India or Sri Lanka where this misinformation is actually leading to death.

The third point on the horizon in the future is regulation. I think there is a real risk of over-regulation in this area. With Europe, for example, and Germany's NetzDG law, I applaud them for trying to take some of the first steps to making this situation better by placing fines on platforms. There has been a lot of, I guess, unintended consequences to that law, and we tend to see a lot more.

To use a good example, as soon as that law was put into place, there was someone from the alt-right party who had made some horribly racist comments online, and it got taken down, which is good, but what also got taken down was all the political satire, all the people calling that comment out as being racist, so you lose a lot of that really important democratic deliberation if you force social media companies to take on the burden of making all of those really hard decisions about content.

I do think one of the threats and one of the challenges in the future is over-regulation. As governments, we need to find a way to create smart regulations that get to the root of the problem instead of just addressing some of the symptoms, such as the bad content itself.

I will end my comments there. I look forward to your questions.

● (1130)

The Chair: Thank you very much, Ms. Bradshaw.

We will go to Mr. Saini for 10 minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you to all three of you for being here today.

Professor Dubois, I'm going to start with you because I read an article you had written with Mr. McKelvey who appeared here last week. You talked specifically about the four different types of political bots. Part of the article was on the amplification and the dampening usage of political bots.

What concerned me with that is that right now you're creating psychographic profiles of people. You're targeting certain people. Information is being harvested. My concern is the dampening of those bots in conjunction with what's being collected. Could there be a possible tactic in suppressing voters?

Dr. Elizabeth Dubois: Yes.

In the work that Fenwick McKelvey and I have been doing on political bots, we identified these amplifiers and these dampeners as the two types of bots that are most frequently used to impact the spread of political information in a way that could be negative.

One of those concerns is voter suppression, because if a "get out the vote" message is targeting a particularly under-represented group within the Canadian voting sphere—we know that new Canadians have lower rates of voting than people who have been here their entire lives—and if there's an amplification of a message that's trying to dissuade them from voting, or a dampening of the message that is trying to encourage them to vote, that could unfairly push them away from participating in their electoral system.

We could also imagine more covert approaches that are similar to the robocall scandal, where we had somebody who created an automated telephone message that directed people to the wrong polling place. You can imagine an automated version of that being deployed on Twitter or on WhatsApp, using automated scripts, which is essentially what we mean when we're saying political bots at this point.

● (1135)

Mr. Raj Saini: You've written that you were in favour of registering political bots, rather than banning them.

Do you think there should be some way of identifying whether a bot is human, so that we can register them by some identifier so people know whether a human or a bot is targeting them? Do you think that would help in any way?

Dr. Elizabeth Dubois: Yes.

I think there are two important pieces to this. One is when I was saying we should register bots, I meant specifically ones that are used to contact voters in the same way the voter contact registry isn't where you have to register every kind of communication a political party has with an individual. The voter contact registry could apply to automated accounts that are targeting people to go to the wrong polling station.

Mr. Raj Saini: If you have certain bots and they're creating misinformation, whether it be racist or threatening information or anything like that, do you think the social media companies have a mechanism in place right now to remove them as quickly as possible?

Dr. Elizabeth Dubois: Yes.

This is where it gets a little tricky. If Twitter, for example, wanted to eliminate all automation on their account immediately, they could, but that wouldn't be very useful writ large, because people benefit a lot from certain kinds of bots.

Think of all the media organizations you see on Twitter. Almost every one of them uses automation to some extent on their Twitter accounts to get stories out on Twitter, Facebook and Instagram simultaneously. That is a form of a bot on Twitter, so I don't think eliminating all automation would be a good idea.

There's also the problem that a lot of accounts are now cyborg accounts. These accounts are automated sometimes, but sometimes a human intervenes and posts content themselves, literally by typing it out and pressing send.

Mr. Raj Saini: Ms. Bradshaw, you've written extensively on social media manipulation and you also mentioned algorithms.

Right now, we're seeing the weaponization of those algorithms. The design was to allow people to personalize their own content, but now they're being used to push disinformation. A solution that has been proposed by the social media companies is to have a separate algorithm to police the algorithms they're using. How feasible is that?

Ms. Samantha Bradshaw: Having the human element in reviewing and auditing algorithms I think is really important. We can't just sprinkle magic artificial intelligence dust on it to solve the problem.

Having this technology support human decisions is great, and that's where I see a lot of the benefit in having a second algorithm, but we still need humans to review this content at the end of the day. There are so many nuanced decisions that these algorithms can or cannot make, and a human making that final judgment is really important.

Mr. Raj Saini: My final question is to you. If you have a political campaign and you have entities, whether it be a third party or political entities that are designing an algorithm to target a certain specific type of voter, do you think that those algorithms maybe should be kept in a repository so that tomorrow, if there is any consequence, then, as you say, humans can analyze that algorithm to see whether there was misinformation or anything that was used in a negative way or—and I don't want to use the word "illegal"—in an untoward way to target specific voters? Then humans could look at that algorithm to analyze whether that was used in a negative manner.

● (1140)

Ms. Samantha Bradshaw: Yes, I think that would make sense. There is always a danger of making algorithms too public, though, because as soon as they become very public and as soon as they're really out in the open there is a whole industry built on trying to break algorithms. There is search engine optimization, so you don't want to make the algorithm so transparent that people can then easily game them.

Mr. Raj Saini: Professor Dubois, do you have any comments on that?

Dr. Elizabeth Dubois: Yes, I think that the ability to game algorithms is a concern when we are thinking, okay, let's create an algorithm to solve this problem and then just make it available for everyone to see. I think that kind of transparency is important, but we also need to have things like published tests of how the algorithms were working, and that can be a way that we can have audits and checks of those systems without necessarily opening the doors up for people who want to then go break the algorithm by circumventing it.

A few of the things I said in my opening statement, I think, connect here. The idea of having a history of the decisions of the people who were on the team who were actually making the algorithm in the first place and learning about what it was supposed to do, and why and how, those are the kinds of information that could help us solve the problem I think you're pointing to in a way that doesn't incentivize people to go and just break everything.

The Chair: Thank you.

Next up for seven minutes is Mr. Kent.

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

Thank you to all for the insight, the opinions and the advice that you've provided to the committee today.

In the barely 24 or 35 hours since NAFTA became USMCA, there hasn't been an awful lot of talk about intellectual property protection and the borderless digital universe. But a number of folks have spoken up and there is some buzz, below the radar, that in fact the protection of Canadian intellectual property will now fall under the U.S. regime, that North America will more or less be under the U.S. system when it comes to the protection of intellectual property.

There is a suggestion that, in fact, the big tech companies will not be responsible for the content on their platforms, which would—it's been suggested, and I'd like comments from the three of you—mean that investigations of the Cambridge Analytica-AggregateIQ-Facebook scandal would not be possible, or that they would be unaccountable with regard to the content on their platforms and the way it's used.

Could we start with you, Mr. Pal?

Prof. Michael Pal: Thank you very much. I think that's an important question.

As you say, it's only been 24 to 36 hours. I did get the chance to look through article 19 this morning, which I think is the relevant one on digital trade or digital policy. There are a couple of things that are relevant there.

One, it does seem to suggest that—and I'm forgetting the exact term that's used in article 19—basically Internet companies, social media platforms, will not be liable under the terms of the agreement for the content posted on them. Now, those things have to be implemented in domestic law and there is what the federal government can do, and what the provinces can do. There are all those kinds of issues there, but that is in article 19.

There is also a provision on source code, which talks about algorithms as well. Maybe I'll be corrected by my colleagues here, but I read that to include algorithms.

Hon. Peter Kent: I think there is a specific point saying that governments will not be able to examine source codes.

Prof. Michael Pal: We couldn't have a mandated algorithmic transparency, but there is an exception for criminal investigation. Would an investigation by Elections Canada or the Privacy Commissioner count as a criminal investigation? That's kind of an open question.

I have no definitive views about article 19. I only read it this morning. I'm going to be lawyerly and cautious and say that I'm not sure of all the implications. It does address and seem to restrict, potentially, in some ways. I suggested liability for social media platforms for repeated breaches of norms around elections. There might be USMCA implications under article 19 that would make that less viable as a policy proposal.

● (1145)

Ms. Samantha Bradshaw: As you mentioned, it's quite new. I haven't actually seen the document yet. I know that social media platforms have always fallen under safe harbour provisions that do protect them from the content that people post on their platforms. Back in the day, we considered it a positive thing because we didn't want to hold Google responsible for someone else uploading content. Google Search would not function, or we wouldn't have it today, if Google was going to be responsible for organizing certain kinds of illegal information.

When it comes to actually holding Facebook accountable with regard to Cambridge Analytica, I'm also not quite sure what the implications of this new agreement would be, but I do think it's a really important question. I'm sorry that I don't have more insight.

Hon. Peter Kent: Thank you.

Ms. Dubois.

Dr. Elizabeth Dubois: Thank you.

I also haven't read the details of USMCA yet, but I think the questions that are brought up are important and we need to look into them.

To build off what Ms. Bradshaw just said, I would say that the idea of platforms being responsible for all of the content that shows up on them has been a major question. As she said, it has been a really valuable tool for the growth of these companies and for innovation in how we deal with the mountains of data and information that now exist, and that's helpful. However, I think that there's an important distinction to be made between allowing content to exist and being responsible for that content, and being responsible for what content shows up as trending topics, recommended search results or something that is at the top of people's newsfeeds.

There are decisions that these platforms make already about what gets the light of day and what doesn't, and those decisions need to be considered in terms of whether or not they are silencing groups that shouldn't be silenced or promoting racist or hateful content that shouldn't be promoted and put forward.

Without having looked at USMCA, I can't tell whether or not that distinction between content and the dissemination of content has been addressed, or the implications, but I think it's an important thing to look at.

Hon. Peter Kent: Some of the early conversation has seemed to suggest that there's a possibility that it would place North America and the protection of privacy in North America at odds with the GDPR, for example, so that the North American regime versus Europe, certainly, and perhaps other jurisdictions, would be at odds.

Dr. Elizabeth Dubois: It seems like it will cost a whole lot of companies a whole lot of money and will be problematic for citizens if that is the case, but I don't know the specific details.

Hon. Peter Kent: Mr. Pal, could I just ask about your thoughts on the GDPR, which came into effect less than six months ago now, but has already affected the behaviour of some North American—particularly American—news organizations by causing them to cut themselves off from distribution in Europe because of fear of prosecution?

Prof. Michael Pal: I think there are some things that we can learn from the GDPR. I'm not even sure that European privacy experts have a really concrete understanding of how it's really going to operate in practice. What does it mean for news organizations? What does it mean for technology companies?

I think what it does point to, though, is that a lot of these tech companies are based in the United States or are based internationally, so in some sense, each domestic state has lost control over some of the conversation around elections. It's not just CTV, CBC and the other domestic broadcasters. I think that it's incumbent on each of the states to try to....

We shouldn't rely on the GDPR, on laws in California or on U.S. federal law. We, as Canadians, have to come up with our own set of rules. I think Professor Bradshaw made the important point that we want to facilitate political expression. We don't want to restrict that. Some of the potential laws you could come up with might restrict political expression. It's a charter-protected right—paragraph 2(b)—and we don't want to restrict that.

Where the charter considerations are lessened, though, is in the area of foreign interference, or foreign actors, individuals or entities expressing views on Canadian politics. Regulating Internet companies or voter privacy in a way that restricts foreign interference, I think, stands on much firmer theoretical and legal constitutional statutory grounds.

● (1150)

Hon. Peter Kent: Is there time for Ms. Bradshaw?

The Chair: There isn't.

Prof. Michael Pal: I'm not critiquing Ms. Bradshaw. I think she made a good point on that, but that's the broader constitutional implication.

Hon. Peter Kent: Perhaps we can get to that later.

The Chair: Yes, you bet.

Thank you, Mr. Kent.

Next up for seven minutes is Mr. Angus.

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

I want to talk about the government's decision not to put the political parties under PIPEDA or a similar regime that would respond to the specifics of the differences between political parties and commercial entities. If you talk to the people around our committee, we're very concerned about this, because we have been looking at the ability of third party actors to actually undermine democracies. If you talk to our political organizers, they're over the moon, because we are now in a digital arms race, and no political party is going to be willing to put down their arms first because they see the potential to do more and more targeting, to get more and more precise, and to shift votes in areas that are key. That's the reality we're dealing with, and we're dealing with a completely different world than we were in 2015 in terms of the speed with which this is happening.

Mr. Pal, I would like to ask you about the importance of having some kinds of provisions in place to make sure that we don't end up misfiring with these weapons, because we've seen what happened in the U.S. and we've seen with the Brexit vote how it can be manipulated. Do you think we need a strong legislative regime, and what would it look like to have some manner of accountability with regard to how our parties and other actors use this information politically?

Prof. Michael Pal: You make a very good point that the scenario in 2019 is very different from what it was in 2015. Things move very quickly, and the risk is that you could put in regulation that is overly intrusive, or that doesn't actually achieve what you want or has the wrong consequences. I'm always aware of that, but I think we have a lot of good information. Political parties are collecting enormous amounts of data, personal data, sensitive data. Parties have always done so, but it's just reached another level. To me this is a non-partisan issue. It doesn't affect one party more than the other, but currently all political actors have an incentive to up their data operations and their data game.

The pitch that I try to make in this space is that actually privacy rules are to the benefit of political parties. No one wants to be regulated, and it may seem onerous and it may cost money, but imagine what would happen if there was a hack of one of Canada's major political parties, similar to what happened with the Democratic Party in the United States. It wouldn't take many hacks, or many instances of personal information being disclosed by, say, a malicious foreign actor for the public to potentially lose faith or trust in that political party or the system as a whole. I think we are at a moment where it's very important to address the privacy issues, and doing so is in the interest of the political parties themselves.

I tried to suggest a few areas in terms of content, such as the right to know what data a political party holds about you, and the right to correct incorrect information. A lot of hard work is done by volunteers, as you all know, and when you're entering information on an app or on a piece of paper, it's very possible for information to be incorrect, and that may be something the voter, the individual, doesn't want. I think rules on who gets access to political party databases or at least disclosure about that might be helpful as well.

I understand those may at times seem onerous to political parties, but I think they go a long way to instilling confidence in voters that the parties have their best interests in mind. The worst case scenario is a hack. We've seen denial-of-service attacks on political parties. I believe the Prime Minister summarized the Communications Security Establishment report, which said there were low-level attacks in the 2015 election. CSE said there were over 40 incidents of interference around the world, so we shouldn't see Canada as isolated from that. I have a lot of concerns about 2019, and I think privacy addresses some of those.

● (1155)

Mr. Charlie Angus: Ms. Bradshaw, I'm very interested in your analysis of junk news. You talk about “cyber troops”, psy-ops, the weaponization of AI.

In 2015, in my region, because I basically live on Facebook, according to my wife, I saw a completely different narrative than what was in the national media. I saw deeply racist posts, mostly from Britain First, anti-Muslim posts, posts attacking immigrants and attacking refugees. They were very targeted. They were targeting on Facebook in key areas of my region among key voters.

It was a completely different message than anything that was happening nationally. It wasn't really noticed, because we still pay attention to what Peter Mansbridge says at six o'clock.

I always felt that out of that there had to have been a better or clearer type of targeting, such that these Facebook users who were not normally political were suddenly repeating this type of message. This seemed to be what we saw out of Brexit, the idea that groups such as Cambridge Analytica can specifically target the poll voters, the voters who are actually going to be influencing, and going on and pushing this.

You talked about how this was used in swing states with certain swing voters. I'd like you to elaborate on that.

I'd also like you to elaborate...because we keep talking about the third party actors as though it's just the bad, hired mercenary guns. You talked about the political influencers who actually are in the parties. Can you talk about the connections between people in the parties, these third party operatives, and how they're using this misinformation online?

Ms. Samantha Bradshaw: If we look at the U.S. and junk news being spread in swing states, this is just based on Twitter. It wasn't a Facebook analysis, but just Twitter and what people were sharing as news and information.

We analyzed a couple of million tweets in the 11 days leading up to the vote. If you looked on average at the URLs that users were sharing in swing states, they tended to point to higher rates of junk news and information, compared with uncontested states. Therefore, part of this is the somewhat organic drive of spreading misinformation. It's not necessarily coming through the advertisements but it's being organically spread through the platforms by users, or maybe by bots, who did play somewhat of a role in amplifying a lot of those stories.

The way we measured where the accounts were coming from was by using geo-tagged data. If a user had reported to be in Michigan, for example, which was one of the swing states, that's how we determined where the information was and where the junk news was concentrated.

There's the organic side of it, but there's also the targeted advertisement side of things. We have a lot of information on Russia, thanks to Facebook's disclosures around Russian operatives buying political advertisements and targeting them to voters based on their identities or values. They homed in on groups such as gun-right activists and the Black Lives Matter movement.

They tended to also play both sides of the political spectrum. It wasn't only about supporting Trump. They also supported candidates such as Jill Stein and Bernie Sanders. They never supported Clinton, though. They would always launch ad attacks on her.

The stuff that comes from the political parties themselves is really hard to trace. That relates back to the question you asked before on laws and what we can do to improve some of this targeting stuff.

We talked to and interviewed a lot of the bot developers who worked on campaigns for various parties. They were the ones who created the political bots to amplify certain messages. It's hard to trace their work back to a political party because of the campaign finance laws that only require reporting up to two levels. Generally how these contracts go out is that there will be a big contract to a big strategic communications firm, which will then outsource to maybe a specialized Facebook firm, which will then outsource work to a bunch of independent contractors. As you go down the list, you eventually get to the bot developer, who we interviewed.

We don't have any specific data on exactly what parties these groups worked for, at least none that I can share because of our ethics agreements with these developers. The big problem here is that we're unable to actually track because of campaign finance laws.

● (1200)

The Chair: Thank you.

Next up is Monsieur Picard.

Mr. Michel Picard (Montarville, Lib.): I need an introduction that may be long, so bear with me.

In my comments, I will disregard and not consider disinformation like calls that send someone to the wrong poll or anything covered by the Criminal Code.

In talking about junk news, fake news, whatever, in the Cold War, and especially in war times, propaganda was one of the best tools in town to make sure that your message, whatever it was, went through. This, and magazines, photos in Middle East countries, in which you see food, everyone at the table, big cars, well-dressed people, just to push the population against their own government....

At the time, sending a thousand letters for publicity, whatever it was, cost a fortune. You had to send one or two pages. Today you send five million to 10 million emails in a click—no cost.

I will submit for your consideration that you are looking at the problem from the wrong end. That's my hypothesis. We try to focus on those who provide this information and bad content, and try to regulate company's social media because they do things that are not good, probably because people are too lazy to do their own cross-checking and verification of information. By the way, we don't prevent people from seeing specific information. We just download a huge amount of information and you don't see where you are anymore.

From a regulatory standpoint, how do you expect me as a government to act on those companies that are sending this kind of content without touching their freedom of speech?

Dr. Elizabeth Dubois: I can start.

I understand that you want to separate things like voter suppression tactics from junk news and junk content. However, when we're thinking about how to deal with one of those things and not the other, it's very difficult to say that we would regulate the platforms only for one thing and we're going to have a completely different solution for the other. The conversations go together, because the mechanisms for getting the information to the front page of somebody's newsfeed are the same.

There's that sort of technical challenge there, but then I think the idea of how we balance this against questions about free speech is a really important one. We don't want to have a democracy where there are people who don't get to share their opinions, where certain views are silenced. That is certainly a problem.

We have to think about the changing media system, though. We have to think about the fact that it used to cost a lot more money and take a lot more resources to spread disinformation. Now it's very easy to spread it.

We also know that people used to not have a whole lot of choices in terms of what content they were getting. For them to be media literate, and not be lazy, in your terms, was a lot simpler. There were fewer checks that they needed to do. There was less work that they had to do to make sure they knew what content was showing up and who created it. There were only so many people who could afford a broadcast licence.

The expectations we put on the citizens in that context are very different from the expectations we would put on citizens now, in saying, “Look, we can't regulate platforms. This is the responsibility of citizens.” In the media environment that we have, I think it's unreasonable to expect citizens to be able to discern the different sources of content, what is true and what isn't, without some support.

I don't want to let citizens off the hook. I think that digital literacy and media literacy are very important, but I think it's one piece of a larger puzzle.

Mr. Michel Picard: Anyone else...?

Ms. Samantha Bradshaw: A lot of it comes down to addressing some of these bigger systemic issues around the platforms. If you can address the root cause of bad information and junk information being able to spread so quickly across social media platforms, then you could also address that while protecting freedom of speech.

Many of the systemic problems, to me, have to do with the whole idea of the attention economy and how, in a world where information is everywhere, attention becomes our scarce resource. Platforms are built on that attention economy. They're designed to tailor content and information and advertisements to us that are going to draw us in, which is what a lot of this junk news does. It's clickbait content. It's designed to get our emotions going and to make us feel angry or happy, to get our attention.

If you can start addressing the way social media tailors content to users by looking at the actual principles that go into their algorithmic design—relevance and virality, for example, are things that are very important to the algorithm right now—and switch those to be principles that would support better democracy, then you can start to regulate the platforms in ways that wouldn't harm free speech.

● (1205)

Prof. Michael Pal: Regulating fake news is the hardest issue. My fake news might not be your fake news. Voter suppression's already illegal. Foreign interference is already illegal, and C-76 takes some really good steps toward closing the final loopholes that are there. C-76 would put in place an offence of impersonating a politician or a political party, so that you couldn't purport that the advertisement came from a particular elected representative or party.

In the Canada Elections Act it's already illegal, if you're a candidate, to claim the person you're running against is going to drop out of the race for some reason. That was a common tactic that was used, so we legislated against it. In C-76, voter suppression and robocalls are all things where we've updated the legislation to deal with whatever the new dirty tricks are, potentially. I don't see any problem in saying, “Today, a lot of the dirty tricks are potentially happening on social media. Which entities have the resources and the ability to actually ensure that the rules are followed?”

It's impossible to try to track down every purveyor of misinformation, disinformation and voter suppression. It's much easier to regulate the social media platforms. It's technologically feasible. They're telling us they're changing the world. They should be able to have a transparency and a repository of election ads without too much of a hit to their bottom lines, and I think we can do that in a way that respects freedom of political expression. One of the things we've learned over the last 18 months is that regulating social media platforms is actually what has to happen now.

The Chair: Thank you.

Next up for five minutes we have Mr. Gourde.

[*Translation*]

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

I thank the witnesses for being here this morning.

I'd like to go back to the roots of the communication problem.

In an election, candidates have to reach between 90,000 and 110,000 electors in a short period of time, in approximately two months. We, the members, have more time because we are already in our riding. If we want to be fair to everyone, that period lasts a maximum of two months.

It is a big challenge, because it's difficult to reach people. Elections Canada provides us with an address and a name, period.

There are two ways to reach the electors, and that is to go door to door or use their phone number, but there are fewer and fewer landlines. All we can do next is try to find cell phone numbers, which is more or less legal, because those are considered confidential in Canada.

Using digital platforms has become a necessary evil for all future politicians if they want to reach a large number of people in a very short period of time. We have less than a 1,000 hours to reach 100,000 people, and that may not add up to a lot of minutes per person. That could be why targeting becomes very interesting to politicians.

Do you think it would be possible to create legislation for these platforms, so as to restrict access to some information, or give politicians more access to these platforms in order to reach people?

If we can't get the phone numbers, we turn to digital platforms. If politicians had access to cell numbers, they could call people and speak to them to at least have some direct contact.

Currently, we are doing politics through indirect contacts. To reach an elector, we are using machines and artificial intelligence, and that is not the essence of democracy. We aren't electing robots, but members of political parties and a prime minister.

The time we have to reach electors is very limited, and I see a problem there for democracy in the short, medium and long term, and that is the root of the problem. Everything else is related to the lack of time and information.

Should Elections Canada provide us with landline telephone numbers and cell phone numbers?

● (1210)

[*English*]

Prof. Michael Pal: One solution might be that political parties should have more consistent information. As you said, the Elections Act provides basic information about name and address. One option would be to provide other information.

You suggested phone numbers. It makes me a little bit uncomfortable.

[*Translation*]

I don't think people would like political parties to have their cell numbers.

[*English*]

I would have to think about that more. If political parties had the right to have greater disclosure about information about voters, then it would be incumbent to have greater privacy protections for that information. If that's a policy direction that the committee is considering recommending, or that you are as an individual, then there has to be a balance there between increased privacy protections and the information that parties have.

Could there be an update on the basic information that's provided? That's an interesting proposal that I had not heard before.

Dr. Elizabeth Dubois: One potential problem with requiring the registration and provision of a phone number is that a lot of mobile applications now connect to people's cellphone numbers, which means that, by allowing or forcing a phone number to be provided, there are potential ramifications for all kinds of different data joining, which would go beyond the ideal of.... A politician or candidate should be able to have that direct communication with constituents and try to engage them in the electoral process, which I think is really good, but I worry about creating a situation where people unknowingly give candidates access to all kinds of information from dating apps to Facebook to their Airbnb listings.

It's not necessarily that the specific listings are going to show up in a candidate's hands, but I think the possibilities for data joining when you use the cellphone number needs investigation. I'm not saying it's necessarily a bad idea, but it's not one I had considered before. My immediate gut reaction is that we need to be worried about the way different datasets can be connected together.

I think your basic point that candidates need to be able to connect with citizens is an important point and, in particular, candidates who are not incumbents end up at a disadvantage if they don't have good enough data to do that basic contact.

Ms. Samantha Bradshaw: I guess I'll just jump in here for the last point.

I definitely agree with Professor Dubois about the dangers of being able to link a phone number, say, to other datasets, because most people do connect their mobile to their Facebook profiles and other social media platforms. There is a real danger there that then you're starting to get more than just the phone number and basic contact information.

I think this does get to the root of one of the big problems we want to address here, and that is the kinds of data political parties should be allowed to use in the first place when they're campaigning and reaching out to voters. Then, what are the limits to that data? I think once we can come up with good answers to those questions, enforce them and create more transparency around this data that political parties have between them and the voters, then that will be a win for democracy.

● (1215)

The Chair: Thank you, Mr. Gourde.

Next up is Madam Fortier.

[*Translation*]

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

I thank all three of you for being here today. We are working very hard on this study, and you have provided us with very relevant information for our work.

Mr. Pal, you mentioned that there were measures in Bill C-76 to prevent foreign or national interference in the elections. What effect could those changes have on third parties? That is one of my concerns.

During the recent election in Ontario, we saw Ottawa Proud, for instance, promote the information of a particular party, and not that of other parties. Do you think that an organization like that one could be affected by a foreign third party or by a government that has a lot of data in its possession?

How can we limit sharing large amounts of data with countries that have fewer regulations, even if financial exchanges are not necessarily involved?

Mr. Pal, I will let you begin, and the other two witnesses may speak afterwards.

Prof. Michael Pal: Thank you for your question. I'm going to answer it in English in order to be very precise.

[*English*]

Bill C-76 closes one of the loopholes that was still existing for foreign interference. It was already illegal for foreign entities to interfere in a Canadian election, but there was a loophole if you spent under $500. Five hundred dollars actually can get you a lot of Facebook ads in some markets. It would close that loophole. That's a very important measure.

How much does it cost to send mass WhatsApp messages or to advertise on Xbox? I don't know the answer to that. Those are emerging uses. Perhaps my colleagues have a sense on numbers. It's not clear how that affects other platforms, but certainly in terms of Facebook or Twitter advertising I think that helps.

I think the information is that third parties are playing an increasing role. There was a much larger number of third parties in the last federal election than there had been in previous elections. I think it's reasonable to expect that to continue. Third parties are basically only heavily regulated in terms of their spending during the election campaign, which is a relatively short period. Obviously you can try to influence voters before the official campaign starts, something that political parties have obviously realized, but also third parties.

I have been an advocate in my academic work for implementing pre-writ...so before the official election campaign rules, some of which are in Bill C-76. The spending limits would apply to what's called “partisan advertising” in the pre-writ period. I really welcome that. I actually think the pre-writ period should be longer. I said that to your colleagues at the procedure committee.

But we have a permanent campaign. Third parties have figured that out. There are other jurisdictions that take an even more aggressive.... Should there be disclosure of advertising by third parties in the full year leading up to the fixed election date? Should there be spending limits? I think there's a really good argument that there should be.

[*Translation*]

Mrs. Mona Fortier: I would like the other two witnesses to have time to answer. I thank you for having told us that.

In your presentation, you spoke about a study you submitted to MIT. Could you send that to the committee?

Prof. Michael Pal: That would be my pleasure, madam.

Mrs. Mona Fortier: Thank you.

Ms. Dubois, would you like to answer my question?

Dr. Elizabeth Dubois: Yes. I also will answer in English,

[*English*]

just so I can be precise.

I think that one of the major things is in addition to what Professor Pal has just put forward about the permanent campaign and where third parties are actually regulated. In addition to advertising and spending, we have questions about data collection itself. It's not just using the data to go and do the targeting, but it's collecting the data in the first place. We see a lot of this happening outside of the election period.

You mentioned Ontario Proud. They registered as an established third party but they weren't an established third party for a large chunk of their lifespan when they were collecting users on Facebook and updating their mailing lists and their text messaging list. That's all reasonable for a private entity or a non-profit organization, or whatever, to want to build up a contact list. But when they're doing that and then using it for very clear and explicit political purposes, that starts to raise questions about our ability to actually know whether or not the people who are in their database and then being sent political content and advertisements want to be there, whether or not the information is reliable, and whether or not the citizens would want to have their data removed. There's no real way that citizens are empowered to take ownership of their data.

● (1220)

The Chair: Thank you, Madam Fortier.

Next up we have Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

When we talk about foreign intervention and potential foreign interference in the 2019 Canadian election campaign, we tend to think of Russia in our discussions. I'd like to ask some questions, however, about the history of the American-based Citizen Engagement Laboratory,which in 2015, in partnership with the Tides foundation, also based in the U.S., moved several million dollars into Canada to Leadnow, or through its Canadian subsidiary, the Tides subsidiary, the Sisu Institute Society in British Columbia.

You mentioned that $500 buys an awful lot of Facebook time, so does $1.7 million or $2 million. I'm wondering about the regulation. We're coming back to third party intervention, where the researcher in British Columbia, Vivian Krause, pointed out that it's easy for a political leader to take the high road in the campaign when a third party is well funded and is doing the dirty work on social media.

I wonder if all three of you could respond to that.

Dr. Elizabeth Dubois: I don't know the details of the Leadnow case. I know only what made the news headlines. I think, however, that it's a very important point when we're having these conversations about personal data use. With something like what C-76 has put forward for the requirements of a privacy statement, which already isn't very enforceable in the context of that bill, and which I think needs to change, it's very unclear how that then plays into the relationship between those parties and the third parties you've brought forward.

I think we need to be clearer about that. I don't have a specific recommendation on how to solve that problem, but I think it's a crucial one.

Hon. Peter Kent: This comes back to the question of foreign intervention.

Prof. Michael Pal: I don't have any information about that particular case. I believe C-76 requires third parties to have their own separate bank accounts, so that is one technical way of addressing the transfer of funds.

Constitutionally, you're on very solid ground to restrict spending. The Supreme Court has spoken about that. As for registration and transparency rules, the Supreme Court has spoken about that as well. There is also the question of contribution limits, in terms of donations to political parties and candidates. What's more controversial is whether you could or should have contribution limits for third parties.

Certainly B.C., in its referendum campaign on electoral reform, has limits on how much you can contribute to an advertising sponsor, and I believe this applies to their provincial elections as well. That does have an impact on political expression if you're restricting how much money.... Say a union or a corporation wants to spend its own money as a third party, how do you regulate that as a contribution? There are constitutional questions there but that's one way of addressing the movement of money between different entities, by treating it like a contribution.

Hon. Peter Kent: As we saw in the Brexit campaign, in the Leave campaign, it's possible to create subsets of the third party to get around those spending limits.

Prof. Michael Pal: If you have contributions being made in really large amounts and you have pre-restricted spending limits that are well enforced, then there's only so much money that can actually be used in that campaign. There's an interaction between the contribution limits and the spending limits.

Ms. Samantha Bradshaw: I'm not an expert on the legal points surrounding what you could actually do to help prevent foreign actors from making contributions to third parties or whatnot. What I do know and what I have seen in a lot of the research we've done tracking foreign influence in other countries is that they tend to work alongside a lot of the nationalist movements that are already in place.

Looking at the U.S., for example, it was always hard to differentiate the language of a Russian influencer from that used by members of alt-right organizations. A lot of that goes hand in hand and they work together to create somewhat of a shared narrative. I do think, however, that there are things we could do to regulate this problem. I think Professor Pal has made some good points. I don't think it's ever going to completely go away, but it's about raising the cost for these foreign and other bad actors. Raising the costs makes it just a little bit harder for them to start influencing voters.

I think transparency around where the funding is coming from, how much of it is spent, and what it's spent on would help create a little bit more accountability in the political system.

● (1225)

The Chair: Thank you.

Next up for five minutes is Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you all of you for being here. Your testimony is incredibly enlightening.

I'd like to take a little step back and get my mind around what exactly we're talking about when we talk about bots, when we talk about cyborgs and when we talk about artificial intelligence. I think we all have a bit of an idea of what we mean but could we look at specific examples?

For example, Ms. Bradshaw, you said that you interviewed some of these bot developers. What does that mean—developing a bot? What goes into that? You said something about how they would have principles, like either virality or relevance, and that you could put principles that support democracy into a bot when you're developing it. Can you explain what exactly that means?

Ms. Samantha Bradshaw: Yes. When I was talking about the principles supporting the algorithms, I was talking more about social media algorithms and the way those things tailor content or deliver content to users. They deliver content based on virality. If things get a lot of clicks, that means that a lot of people find this really interesting and, therefore, it might trend. That's sort of what I was talking about there.

Instead of principles around virality, maybe we want principles on factual information coming from professional news outlets as opposed to sources that constantly produce misleading or fake news. The professional news should maybe get—I can't think of the technical word right now—but it should be prioritized in the algorithms. That's what I was referring to there when I was talking about designing algorithms for democracy. It's changing those sorts of principles.

When it comes to the actual bot developers.... This wasn't my core research project but I could point you to one of the researchers who did a lot more of these interviews than I did. His name is Sam Woolley. What he found was that the bot developers are just like any other tech developer. They're creating a piece of software that is designed to mimic human behaviour. It might amplify a certain story. It might converse with actual users online.

Bots do a whole bunch of different things. It really depends on what the goals of the developer are. The developers might actually have ideals or principles that they feed into the bots. A lot of them see these bots as being good for democracy because they're helping to amplify a message that might not get heard or go trending without the help of the bot.

Ms. Anita Vandenbeld: Ms. Dubois would like to speak.

Dr. Elizabeth Dubois: Political bots are automated accounts, sometimes found on social media, sometimes found on Instagram, sometimes found on Twitter, sometimes found in instant messaging apps. There's a bunch of different places where political bots are interacting.

There are other kinds of bots that make use of digital data to do things like make sure Wikipedia is up to date. There are different kinds of bots, but typically when I'm talking about political bots I mean these ones that are interacting with humans. They are mimicking humans in some way. The people creating those bots may have a lot of technical skill. They may be computer scientists and developers. They could also be people using tools that have been developed by some other developer to quickly create bots. You don't necessarily need to have a lot of technical skill to get a bot up and running.

We also need to remember that there are entire companies—in fact, an industry—built around the idea of search engine optimization that uses some of these techniques and could make use of a bot network they created. For example, there could be a whole bunch of bots they create say on Twitter to all interact with each other to amplify a message. There would be an organization potentially behind the development of those bots, and you can trickle down, as my colleague was explaining, to the specific person who was the original writer of the code.

● (1230)

Ms. Anita Vandenbeld: One of the things you mentioned, Ms. Dubois, was people who would game the algorithms. I think you even referred to breaking an algorithm. What does that mean?

Dr. Elizabeth Dubois: Gaming an algorithm would be.... The typical example is search engine optimization. Another way is, say, we have an event happening in Ottawa. We want the hashtag for that event to trend in Ottawa so that anybody in the Ottawa area sees the hashtag on their little trending bar on Twitter. The idea might be to create a whole bunch of bots that share content using that hashtag to artificially bump up how important it is on Twitter, so that Twitter's trending algorithm forces it to be front and centre for people to see. That would be a form of gaming the algorithm.

Breaking it would be gaming it to the point where the company that created the algorithm in the first place has to revamp it entirely because it's no longer doing what it's supposed to do.

The Chair: Thank you.

Ms. Vandenbeld, that's time.

We're going to do another round after this, but the last three-minute round goes to Mr. Angus.

Mr. Charlie Angus: Thank you.

What started this whole investigation was the massive Facebook breach that led to Cambridge Analytica and the potential that that information undermined the Brexit vote. There was another Facebook breach of 50 million users. We have no idea. We're told not to worry. As far as they can tell, everything's fine.

As soon as I heard that, I thought, “Wow, thank God we have Facebook on the case. There's nothing to worry about here.”

When we had Facebook here, we were asking about the mass murders that happened in Myanmar. It's not the responsibility of Facebook that there were mass murders, but Facebook was accused time and time again of not responding to the misuse of their platform. Their response was something like, “We admit it, we're not perfect.” We're talking about the power of a platform to engage in mass killing.

We're talking about a lot of tweaks to a system that suddenly seems more powerful, more encompassing than domestic law, than anything we've dealt with in the past, and that seems to be moving beyond many jurisdictions with very little regard. Do you believe that platforms like Facebook, like Google, need to be regulated, or can we trust them to respond when there's enough outrage? Does there need to be antitrust action taken to break them up, since Facebook now controls Instagram, WhatsApp, and many other platforms? Google is the same.

What do you see in terms of holding these companies to account? Is it self-regulation? Is it antitrust? Is it some form of national or international regulation? I put that open.

Ms. Samantha Bradshaw: I'll jump in here first. For me, it's a little bit of everything. We definitely need regulation. If the past year has taught us anything it's that we need to step in, and government has a really important role to play in regulating these platforms.

I think private self-regulation is also an important thing to address here. For your example with Myanmar and how Facebook caused a lot of fake news and misinformation to spread, leading to violence and death, I think that's a real, serious problem. Like you said, we have these companies that operate globally, but they don't have staff working in each country on the content moderation side to address a lot of the very local problems.

Having a content moderator sitting in California who doesn't know anything about the history and culture of Myanmar or Sri Lanka, or a lot of these other countries where there are ethnic tensions, making decisions about content is a really big problem. Yet Facebook has advertising staff in a lot of these countries, so I think stepping up on their content moderation and making it more global and inclusive is a good private, self-regulatory step that governments could also push onto the platforms.

● (1235)

Dr. Elizabeth Dubois: I think self-regulation is absolutely insufficient. What Facebook in particular has been doing in reaction to the pressure now being put on them is good. We need to continue seeing those things.

Professor Pal brought up the example of making a repository of some election advertisements available voluntarily. Yes, that's great, and I am happy that happens, but as Professor Pal also mentioned, they could take that away and we would have absolutely no recourse. Elections Canada would then be left vulnerable because they decided to rely on something that was not legally mandated. If that's taken away during an election, we have a huge risk to our democracy and our democratic system.

We also need to remember that these are major international companies. They are not going to have the specifics of the Canadian population in mind when they're designing their self-regulation. Thinking about the Canadian population, we have large parts of the northern bit of Canada that are very reliant on Facebook as their main source of connection to political information. If Facebook is not actually able to pay attention to the nuances of aboriginal populations in Canada and the ways they share information, then those people are potentially underserved in a way that is counter to our democracy and potentially really marginalizing.

Why would we expect the people at Facebook who are making decisions about how Facebook will roll out all across the world to understand the specific Canadian context in those particular areas? That would be unreasonable, I think, to place on them and just say, "Oh yes, they'll take care of it." In fact, we need the Canadian government to be the one standing up for Canadian citizens.

The Chair: We're at the end of our first round.

I'm going to ask a question to the panel, if I may.

One thing we've talked about in the past is anonymous accounts on Facebook and the platforms that.... They hide in the shadows. They're bots or they're real people who hide in the shadows, or whatever. Should it even be possible to hide in the shadows and not be a public entity? That to me seems like it would be an obvious place to go. An algorithm couldn't impersonate somebody who just isn't there, if they weren't there. It would have to be a real person attached to that particular file or particular program, etc., actually using it. Do you see that as even possible, or is that a place to go? What are your thoughts on that?

Dr. Elizabeth Dubois: One of the major problems with having what we would maybe call an "identity layer" like that is what becomes the verification of real personhood. Airbnb asks you to take a picture of your passport or your driver's licence. I'm not super comfortable with Airbnb having a copy of my passport when I logged in through Facebook and then 50 million user accounts' information has been accessed. There are major implications there that could be really problematic in terms of privacy and personal data security.

There are also questions about whether anonymity would actually fix some of these problems. Nathan—I forget his last name—he is is at MIT, wrote a really interesting review of the role of anonymity and whether it helps in cases of hate speech and disinformation. In fact, getting rid of anonymity largely wouldn't solve those problems, so that's potentially problematic as a solution.

The Chair: Ms. Bradshaw has something to add.

Ms. Samantha Bradshaw: I agree. I think there is a real risk in removing anonymity from these platforms. We do have to remember that they are global platforms. Protecting the identity of individuals in countries where there is less freedom of speech and less protection against violations of human rights.... People rely on anonymity on these platforms to communicate, to deliberate and to organize protests.

I could relate this to Twitter's little verified accounts. If, say, accounts were verified as being those of a real person, that could make fake accounts even more powerful, because they have now passed that filter and people will tend to trust those sources more. They could actually be more effective at spreading disinformation.

● (1240)

The Chair: That's interesting.

Mr. Pal.

Prof. Michael Pal: I think the proposition that anonymity can be important in facilitating political expression is a really good point. I think that applies in Canada too, in certain circumstances. I would draw the line where, if you're spending money on something that counts as election advertising under the definition of the Elections Act, then there should be some verification of the source, that it's a real person and a domestic actor who is behind it. It's different if you just want to express yourself, say, politically on Twitter and criticize a politician. There is value in allowing anonymity there.

That's where I would draw the line. That can be a difficult one to enforce, potentially. If you're spending money on advertising, then the public should have a right to know.

The Chair: Thank you.

First up for the next set of questions I have Mr. Baylis for seven minutes.

Go ahead, Mr. Baylis.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): I'm going to start exactly where you finished, Mr. Pal. I'd like all three of you to answer this. I'm going to start by trying to do what you said, Professor Dubois, define a political advertisement.

I see it two ways. If I've stayed in my house and written an article and put it out on Facebook or Twitter or whatever, and people start sharing it, whether I have 100 friends or 10,000 friends, I've just put it out there. If I take the same article and pay $10 to have it posted somewhere, I make the argument that this has now moved from a personal posting to an advertisement. I'd like to hear if this is a first line of delineation that we could do to say, "This is an ad. This is not an ad."

Maybe, Professor Pal, you could start with that.

Prof. Michael Pal: There is a definition of advertising in the Elections Act: advocacy for or against a political party or a candidate, directly or indirectly, or on an issue they are associated with. We can work from there.

Mr. Frank Baylis: But the delineation on being paid or not...?

Prof. Michael Pal: Some systems, a federal one, has a monetary amount, so Bill C-76 is going to eliminate that for foreign entities' advertising but it would still be there for domestic entities. B.C. did not have a monetary amount and there's a recent case in front of the Supreme Court of Canada trying to interpret what it means if you buy crayons and your kid puts up a political sign in the window, so having some kind of a monetary threshold I think is useful. It potentially stops over-enforcement of small political advertising.

Dr. Elizabeth Dubois: I think paid content versus unpaid content is a useful distinction. I think we also need to remember though that the content is important in deciding whether this is political or not. It's the dissemination of the content that makes it the advertisement. You could pay an artist to create a political campaign message that you leave in your house. That's paid and it's political but it's not being disseminated to others. The distinction there is important because things that help disseminate content that was not paid, I think, could reasonably still be considered an advertisement.

Imagine somebody writes a post on Twitter, they themselves don't pay to have it promoted, but somebody else chooses to promote it—

Mr. Frank Baylis: I want to come back to that, but let's just start with them first of all.

The first act is that I write a post and I put it on there. I have not advertised if I've not paid.

Dr. Elizabeth Dubois: Right.

Mr. Frank Baylis: I'm going to come back to that second point.

Professor Bradshaw.

Ms. Samantha Bradshaw: I won't add much to the conversation here other than that I think the differentiation between something that is paid for and something that I post organically is a good way to define an advertisement.

Mr. Frank Baylis: Okay, then swing back to the second step. First of all, we say there's a monetary threshold. Now that threshold maybe should be brought down because its impact could be higher. We say, "This is a paid ad. This is not a paid ad." Suddenly someone comes along with a bot and says this guy wrote a great article in his house and he shared it with 10 friends and we want to get this message out there. So the bot goes to work or I start paying. Then I've converted it into an ad at my stage, or even if I just told a bot to search the Internet, find this good stuff and then stick it out there, then that translates it from being a non-paid ad, when I put it up there, to now being computer driven.

Would that also be where we could say this is now a paid ad?

● (1245)

Dr. Elizabeth Dubois: Perhaps Professor Pal would have a better sense of whether under current law that would be the case. I think it should be, the caveat being it wouldn't be the person who created the content in the first place who should be held responsible, but instead, whoever has paid for those bots to be directed at that content.

Mr. Frank Baylis: You're saying the person who has converted something into an ad.

Dr. Elizabeth Dubois: Yes.

Mr. Frank Baylis: All right.

Professor Pal.

Prof. Michael Pal: Elections Canada has an interpretation note on political advertising online. It says that to count as election advertising, the item must have a placement cost. The legal question is whether there was money and transmission, but there also has to be a placement cost, which is different from, say, on television or radio. I guess the question is whether it counts as a placement cost or not.

We want to be cautious that we don't restrict the ability to share information organically.

Mr. Frank Baylis: We're not sharing it organically. We're saying it has moved from being organic to being professionalized. Once a bot comes in or another person is paying, we've now moved it from organic to professionalized. In that instance, you're saying there is a placement cost.

Let's say I designed an app and I put it out there, and it was just doing its own thing without me. Would it be covered by this placement cost, or should we adapt the law?

Prof. Michael Pal: I would want to know more about the facts, but I don't believe so. The placement cost regime doesn't work perfectly when we're talking about bumping up posts and sharing through bots or cyborgs.

Mr. Frank Baylis: I call it professionally sharing, as opposed to letting it happen organically. Let's forget Facebook exists and say, for example, I talk to my friend. He says that's a great idea, Frank, and he talks to his friends. There's nothing against the law there.

Now, let's say we've defined what an ad is and what it is not. There are a number of things you've all mentioned around controlling an ad. I don't have much time, and I agree with the public repository. Does anybody disagree with that? Okay.

I agree with listing who the official agent is, and who paid for it. I agree with the idea that the advertising rates should be the same as we have now, so they can't inadvertently promote one point of view.

You put forward one area where I'm not in agreement, which is transparency in terms of why the voter was targeted. Let's say I go back to soap operas. Soap operas came out in the 1930s. People had radios, and advertisers asked themselves who they were going to target. They wanted to target women, because women were going to stay at home. They wrote the content for women, and they put it on when they knew women were home alone. They were selling them soap, hence the name soap operas.

I don't see the problem with someone targeting me per se. I want to hear your thoughts on that, starting with you.

Prof. Michael Pal: The public policy issue is that voters might feel deeply offended by the specific search terms that were used to target them. Part of the reason that has purchase is that those individuals don't necessarily know what data the entities that are advertising to them have.

It's very hard as a user of Facebook to know what information Facebook has about you. It turns out if you were logging in to Facebook using two-factor authentication, they were using that and giving additional information to advertisers. That's what we learned in the recent breach affecting 50 million people or more. It goes to the idea that you should have as much information as possible regarding how you are now being included in the political process, and because there's a public interest in having political advertising that works on terms that we agree are legitimate in a democratic system.

If you're selling shoes, it doesn't bother me as much what search terms were used. If you're targeting people because you think they are racist or you might be able to encourage them to be more racist, you can't do that on an ad on *Hockey Night in Canada* because you're going to get called out on it, right? Everybody else sees it.

However, if it's microtargeted to an individual, you don't have that public element, so it behooves us to give more information to the individual, to enable them to make that assessment.

The Chair: We're actually out of time. I'm sorry, but we're really tight for the last seven minutes. I have to move on.

Mr. Kent, you have seven minutes.

Hon. Peter Kent: Thanks very much, Chair.

I've been impressed that all of you have said in different ways today that we should be cautious about over-regulating with regard to the digital world, social media and accumulated individual data in the elections process. I'm wondering how much transparency should be made available to individual voters about what political parties have on them or what political parties consider their voting inclination to be.

After all, door-knocking, face-to-face contact, is still here today. It used to be telephone as well, but with the absence of land lines that's pretty much gone the way of the dodo. When we knock on doors throughout one riding or another, we find out who is inclined to vote for the party during the writ period or during the entire parliamentary session.

On election day, we're interested in getting out the vote, so our encouragement, our messaging one way or another, is to those who we know are likely to support whichever of our parties exist. It's not that we're discouraging others who at the door have told us that they're not voting for us but for party X or party Y. It's simply that we go where the votes are. We don't waste our energy trying to encourage people at the moment of decision to go to the polls and vote for us.

Again, coming down to the thorny concept of who owns my identity in the digital world or the accumulated data world, would it be necessary to tell a voter that we would consider them to be unenthusiastic about supporting me as a candidate or perhaps even hostile and very unlikely to ever vote for me or my party? How would one divulge that information? Also, wouldn't there be an awful lot of make-work if everyone is demanding to know what the party thinks of them or how they consider them?

● (1250)

Dr. Elizabeth Dubois: Yes, I think this is an important question. On the comparison to the data collection done now versus how it was done when door-knocking and phones were really the only option, then people knew at some level what data was being collected on them because they were asked. They had to actually give it to somebody to write down on that clipboard.

Hon. Peter Kent: Yes.

Dr. Elizabeth Dubois: That's an important distinction. The idea of whether this is going to make a whole lot of work that's going to tax parties in ways that are unfair is important. At a minimum, what I have suggested as necessary would be the top level.... It would be saying that as a party this is the data we're collecting and these are the sources, so we're collecting information about who you say you're going to vote for if you offer it up, and we're collecting information about what your phone number is, and this is how we're going to get it. You're listing that out.

Then, in terms of having a mechanism for people to go and check what that is and correct information that's wrong, I think that becomes a bigger question, where we start to get into things like whether we want to take the GDPR approach. Is that what Canada should be working towards? I haven't been an expert on GDPR, so I can't really speak to the specific implementation of that, but from the perspective of a political party personal data privacy statement, I think having a minimum statement that "this is the data we're trying to collect about you and this is how we're going to get it" is important.

Prof. Michael Pal: I think privacy protections for voters are important. It is fair for political parties, though, to say that they need some mechanism to weed out frivolous or vexatious demands that are simply there to take up all the political parties' resources. You can imagine another political party sending out a bunch of people to request their personal information every day, right? That's not too fanciful a scenario.

Most other entities in Canadian society that have significant amounts of data do comply with the privacy rules. It's a good question in terms of how exactly to design them. I think it's fair to weed out the frivolous ones, but I think it can still be done for political parties.

Hon. Peter Kent: Professor Bradshaw?

Oh, we've lost your audio.

Ms. Samantha Bradshaw: I missed most of that question, because the call cut out. Would you mind just summarizing quickly?

Hon. Peter Kent: How much information would you expect political parties, individual political campaigns, to divulge about what they know about a voter's either being in support of that party or candidate, or against?

Ms. Samantha Bradshaw: Whatever political parties are collecting on potential voters, it should be divulged. As some of the other panellists have said, other entities do report that information under law already, and political parties should not be an exception here. It's really important that users also understand that this is the data these entities have about them.

● (1255)

Hon. Peter Kent: The problem is that when you knock at a door, sometimes you get an enthusiastically supportive response or sometimes you get a quite strongly expressed negative response, but I would say that in many elections you get the undecided, and there are shades of undecided: "Well, I'm interested", or "I'm leaning...", and so on. This would come down to the nomenclature of how parties would be required to log the face-to-face contact they're getting and how to express it to people without being either offensive, or as professor Pal suggested, subjecting them to vexatious inquiries for days and days just as a time-consuming, resource-consuming exercise.

Ms. Samantha Bradshaw: Where I would like to see improvements here comes down to the reporting on why I would be targeted in the first place, because compared with knocking on doors, or even using other technologies such as television or radio, that kind of interaction doesn't provide the same wealth of information that social media collects about individuals. To put this into your monetary context, Google just paid $9 billion to have Google Search be the default on Apple devices. That's how valuable the data that's collected about us on these platforms really is. It can say a lot, and that's why I think having more transparency as to why we're being targeted, for what reasons, is really important. It does change people's decisions.

The Chair: Thank you, Mr. Kent.

Last up is Mr. Angus.

Mr. Charlie Angus: Thank you.

This has been fascinating. As you can see, we're dealing with a very unwieldy subject. We want to get this into a report that we can present to Parliament with timely suggestions that are not interfering with the right of people to fight with each other on Facebook or troll politicians that they don't like. That is a democratic right. We also want to make sure the rights of people are not being unfairly interfered with through data manipulation.

You've all brought forward some very good overall recommendations, but are there specific recommendations that you think we should consider for our report? If you would put that in writing and send it to us, it would be very helpful, because I think we're moving towards coming forward with something we want to present to Parliament. Your recommendations here have been excellent, but if there are specifics, please, send them to us.

Thank you.

The Chair: I'll just follow up with what Mr. Angus has asked you. Please pass any ideas and suggestions on to us, and we'll try to have them included in the report for what we see as the future for our democracy.

As chair, I want to thank you all for appearing today.

The meeting is adjourned.