HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 116 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, September 25, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, September 25, 2018

● (1100)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I will call the meeting to order. Welcome back, everyone.

This is the Standing Committee on Access to Information, Privacy and Ethics, meeting 116, on the breach of personal information involving Cambridge Analytica and Facebook.

We're going to start off with our teleconference witness. Welcome, Mr. Owen.

Professor Taylor Owen (Assistant Professor, Digital Media and Global Affairs, University of British Columbia, As an Individual): Thanks for having me.

The Chair: Go ahead. You have 10 minutes.

Prof. Taylor Owen: Thank you.

I think I want to leave you with one message today in my opening remarks, and that is that I really believe that the issue you're diving into of the particularities of the vulnerabilities that were shown and demonstrated through the case of Cambridge Analytica's use of Facebook and collection of data about American and Canadian citizens is not a case of individual bad actors that need to be countered, but rather is a function of structural problems in our very digital infrastructure, which I think are creating weaknesses in our free and open society. These weaknesses, I think, are being exploited by corrupting the quality of information in our public sphere, which is increasingly digital, by magnifying divisions in our society and by undermining our democratic institutions themselves. I want to talk about those problems and the structural elements of these problems by making four points over the next few minutes.

The first is that I think it's really important as a baseline to recognize that there has been a real evolution of our digital infrastructure, particularly of the Internet, over the past 30 years. In very broad sweeps—obviously, this is a much more detailed evolution—the first iteration of the Internet, web 1.0, really did give voice to a whole host of actors and individuals and groups who were excluded from our mainstream public discourse.

Web 2.0, in the 1990s and 2000s, the social web, connected people in really powerful ways and often democratizing ways, as we saw through the Arab Spring and through a whole host of social movements that leveraged these technologies around the world in incredibly positive ways.

I now think that the Internet is something qualitatively different. The problems you're investigating are representative of this difference. I think we're in a third phase of its evolution, what I broadly call the platform era. I would argue that this current version of the Internet is largely controlled by a small number of global platform companies, and for many people in the world the Internet they experience is filtered via these platform companies. That's what I want to talk a little bit about today.

The second broad point I would make is that in this platform ecosystem, this platform Internet, there are two structural problems embedded in that very Internet infrastructure. The first is the way that platforms or the Internet or we have been monetized—what's often called the attention economy or surveillance capitalism.

I would argue that in this tightly controlled market for our attention, audiences can be microtargeted and behaviour can be nudged by anyone from anywhere for any reason. Our attention and our behavioural change is the product being sold in this digital economy.

At the same time as our microtargeting behaviour is being affected or changed, since engagement is the primary metric of value in this attention economy—how much we engage, whether positively or negatively—platform algorithms prioritize entertainment, shock, and radicalization over reliable information. This is embedded in the business model. This is why research shows, for example, that misinformation spreads further and faster than genuine news. It's because it's embedded in the model.

The second structural problem, I think, which we're on the front end of and is going to become a much bigger issue over the coming years, is that the character and what we experience in this digital platform ecosystem is increasingly determined by unaccountable artificial intelligence systems.

These AI systems are used to filter the most engaging content to us, to know what will rile us up and engage us, to determine what we see as an individual user and whether we are seen and heard inside these platforms. Increasingly, AI is used to create versions of reality itself. They're often called deep fakes or synthetic media. A whole new reality is shaped by AI and targeted specifically to us as individuals.

● (1105)

Those are what I see as the structural problems here.

The third point I want to make is that I think these structural problems are responsible for the negative externalities we're now seeing in our democracy, one of which is represented by the Cambridge Analytica case and the 2016 U.S. election, but I think these negative externalities extend far more broadly. Let me describe a few.

One is that the quality of the information we receive, or the information in our digital public sphere, is becoming increasingly unreliable. The platform web is increasingly a toxic place. Highly gendered and racialized speech is incentivized, political discourse has become more extreme and divisive, which you experience intimately, and speech has been weaponized, with a resulting censoring effect. Voices are simply drowned out by abuse. At the same time that this is happening, the digital public sphere is becoming more toxic. We're seeing the increasingly rapid collapse of the industry of journalism, providing weaker and weaker backstops against this flood of false and toxic content.

In my view, democracy requires a grounding of common and generally trustworthy information, and I fear that because of this structural problem this is slipping away from us.

The second negative externality I want to mention is fragmentation. On platforms, we're each given a customized diet of information designed to reinforce and harden our views. The result is that polarization and tribalism can very quickly emerge in this ecosystem. This is a problem for a wide range of reasons, but perhaps most worryingly because it's increasingly leading to actual physical manifestations of individual and collective violence.

A recent study found that in any German town where per-person Facebook use rose to one standard deviation above the national average, a tax on refugees increased by about 50%. I think that Canada without a doubt lags on some of these trends and the social implications of them that we've seen in other western democracies, but fragmentation based on unreliable and microtargeted information is sure to divide us on the issues that are most poignant in Canada now. Imagine climate change, indigenous rights, pipelines and immigration all being fuelled by this structural vulnerability.

The third negative externality, which I think is of acute interest right now in Canada, is the vulnerability of our elections themselves. I would argue that by using the very tools provided by the attention economy, foreign and domestic actors alike can powerfully shape the behaviour of voters. AI and data-driven microtargeting is incredibly powerful during elections, as we saw with the Cambridge Analytica case. Acute cyber-attacks and hacking are a vulnerability, as we saw during the Clinton email leaks or the Macron leaks, but I think you can also be more subtle. I wouldn't want to focus too much on just these very acute public cases.

I can give you an example of a more subtle case. A recent study found that long before the 2016 U.S. election, Russian government-connected accounts created a host of fan pages on Facebook for prominent African-American figures. They did one for Beyoncé and one for Malcolm X. The goal was to build an organic community. They published fan content about Beyoncé to try to build the followers of that page. In the days before the election, they then weaponized that community and pushed content to them designed to suppress the African-American vote.

How do we deal with something like that? How do we even know that this is a foreign-sponsored fan page and that it will be weaponized in the days before the election? This gets at the real structural problems we're facing here.

In the final and fourth point I want to make, I want to offer a few reflections on the public policy solutions to this problem or the governance challenges that this presents.

The first point I would make about public policy here is that it's very clear that self-regulation has proven and will continue to prove insufficient for the nature of this problem. I would argue that the apt analogy is the lead-up to the financial crisis, where the financial incentives are powerfully aligned against meaningful reform of the ecosystem. These are publicly traded and largely unregulated companies whose shareholders demand year-on-year growth.

● (1110)

This growth simply may or may not be aligned with the public interest, and that's how democracies function. When there are negative externalities of largely unregulated monopolies, governments engage to protect the collective good. I think that's where we are now.

I have a second point about public policy here. To me this is primarily a demand-side problem that requires a comprehensive policy approach. Many have argued that it's actually the users' fault, that it's a supply-side problem, that we're consuming and producing toxic content and therefore we should change consumer behaviour. I actually think that misses the structural aspect, and indeed, almost every major global commission or report that has looked at this issue has argued that a comprehensive policy approach is needed. There's not just one silver bullet to this. It's about reforming how we regulate and engage with our digital economy writ large. This is going to involve—

The Chair: Mr. Owen, you're at just about 11 minutes.

Prof. Taylor Owen: Okay. Sorry to be—

The Chair: We'll get back to you with some questions maybe, if you want to continue a little later.

Prof. Taylor Owen: Absolutely. Let me just finally conclude here, and Ben's going to talk about these policy proposals, which I agree with. They're going to involve immediate fixes such as ad transparency and new data rights regimes, regulatory changes to give rights to Canadians over the data that's collected about them, and reform of our journalism space and the way we regulate the journalism space.

I'd be happy to talk about any of those afterward.

Thank you.

The Chair: Thank you, Mr. Owen.

Next we have Mr. McKelvey for 10 minutes.

Professor Fenwick McKelvey (Associate Professor, Communication Studies, Concordia University, As an Individual): I'd like to begin by acknowledging that the land on which we gather is the traditional unceded territory of the Algonquin Anishinaabe people. Further, I'm on parental leave now, and I would like to thank my family for giving me the time to speak here today.

I hope my comments will be relevant to the committee and provide evidence to support its preliminary recommendations, which I largely support as well. I appreciate its willingness and dedication to keep pulling a lone thread that unravels this tangled web of data, surveillance, campaigning and advertising. These issues have been a great preoccupation for me, bringing together previously separate research into Internet policy, digital political communication, and algorithmic governance.

I would like to focus my comments on three areas of investigation before the committee today. In many ways, they complement some of the findings and conclusions of Taylor Owen, such as the focus on online advertising, third party data brokers and analytics, and finally political parties. My comments highlight my concerns and potential policy remedies to these issues based on my own research. I hope the committee will also look to new ways to support more research in these areas, giving researchers better access to data under clear ethical guidelines.

First, online advertising is more than a political problem. The Cambridge Analytica Facebook scandal has exposed more than anything the public's unawareness, resignation or willed ignorance about the sophistication of online advertising. It might not tip the next election, but reforms to the sector will go a long way toward restoring public trust in the Internet writ large—speaking to the structural issues of the presenter before me.

Online advertising means a few things today. It concerns programmatic banner advertisements of the kind we see around every website. These ads account for a $12-billion industry in Canada, according to the Media Concentration Research Project, and Google and Facebook account for three-quarters of the revenue. However, there are new types of advertising. Native advertising, or sponsored content, confuses the line between advertising and advertorial. With influence marketing, informal brand ambassadors fill our social media feeds with their often unacknowledged endorsements. There's also spam and bot activity.

In general, I question the public benefit of all these forms of targeted advertising. In my mind, we have too little accountability and too much in the belief of data and targeting. New kinds of advertisers will present problems for political campaigns. Political campaigns may turn to these grey markets, using influencers or “for rent” social media accounts to fake grassroots support. We must recognize the extent of this promotional content in our culture, make steps to be able to qualify it, and also work to ensure proper disclosure and fair play for these third party advertisers. One tangible step might be to work with Elections Canada to clarify the placement cost criteria to ensure that the new types of advertising count in electoral spending.

In regard to programmatic advertising, we need to consider what are appropriate limits to data collection and targeting. There's evidence in the political literature that the multitude of microtargeting does not necessarily help campaigns better engage with voters. In my opinion, the current situation overstates the value of targeting data, omitting the potential harms in over-collection. We can name a few risks of over-collection. Conceivably, we can think about advertising profiles being used as a proxy for protected categories like race and political belief. Targeted advertising is increasingly used to justify growing online and offline surveillance. Finally, all this data can be leaked or improperly handled, as we've seen time and time again.

Data protection is an important remedy. By limiting what can be collected and used for targeting, we can diminish the race to monetize more personal information for advertising. Without change, I fear a time when large social media companies compete against Internet service providers on how much data they can collect and turn into targeted advertising portfolios, collecting as much data as they can.

AggregateIQ is part of a global technology industry. Canada, like many other western democracies, has witnessed political parties go digital to better run their campaigns. Many companies now sell services to help parties manage, analyze and use their data to, among other things, buy ads and gauge support.

For its proponents, technology-intensive campaigning gets out the vote. It also helps parties find the right supporters, be more responsible with their limited funds, and ultimately win. I do not dispute these claims, but it has become clear to me that the global scope of the industry today creates new regulatory challenges, particularly in ensuring that offshoring data analytics or digital services does not evade national spending or national privacy law.

● (1115)

These industries warrant greater scrutiny, particularly in how they move data across borders. Offshoring data analytics should not evade privacy laws. International companies should be mindful of how they transport models, particularly models using machine learning algorithms that might have been collected and developed using loose privacy laws, and make sure they do not find their way abroad.

I believe these issues can be addressed by adding enforcement powers to the office of the Privacy Commissioner and continuing to support its multi-jurisdictional enforcement.

Third and finally, with regard to political parties, I was not surprised that AggregateIQ has little uptake in Canada. This is not because there is an aversion to technology in politics but because parties already have their own solutions in place. The Conservative Party uses NationBuilder, together with its proprietary database. The Liberal Party uses the U.S. Democratic Party-affiliated NGP VAN. The NDP works with other Democratic-affiliated firms, Blue State Digital, and its own tool, Populus. I have to admit I'm surprised that no representatives from these political parties or from these companies have appeared before these committees investigating these matters of political data.

In general, political parties have much to do to be more accountable about their data habits. Again, in my research I've been impressed by the professionalism of campaigners on all sides, and I believe these professionals will ultimately embrace these new rules. I understand reluctance, too, to impose more regulation on already taxed organizations, but greater accountability for digital campaigning should benefit all parties.

I support the committee's recommendation for privacy laws to apply to political parties. I'd like to add one other reason.

In my own research I've found that lax rules have created real challenges for political campaigns. Data is a strategic resource for parties. Lax rules, however, translate into real inequities. Incumbent parties have better access to data than new entrants. To compete, all parties have to be constantly maintaining their lists and collecting more data, since they cannot rely on the data collected by Elections Canada. This leads to an overall concentration in the central party, which often becomes the database, and an overall logic of permanent campaigning.

Parties might be reluctant to adopt privacy law, given the importance of digital fundraising. If we believe that parties should collect less data, then we may want to consider reinstating the per-vote subsidy that diminished the need for funding and its associated data collection.

Also in terms of data, most parties use some form of predictive analytics to examine the political data they have collected and make predictions about voter behaviour. Either the party or, more often, the consultant analyzes the data to calculate the probability that each voter will support the party and the probability that a voter will be persuaded to vote for the party. The parties use these to make important decisions, like who to target and who to encourage to vote. Predictive analytics exacerbates low voter turnout in Canada, allowing parties to continue to distance many voters from the electoral process. Parties should agree to audit their scoring of voters, and other analytics, for potential race or gender biases. As well, they should also make sure that these decisions about which voters to contact and which voters to ignore are auditable and explainable.

Finally, my suggestions about reform to digital campaigning are my own experiences alone.

Political parties ultimately need to work together on the rules of the game. Codes of conduct have long been recommended to improve Canadian politics. I believe that now is the time to move toward the drafting of a code. In many ways, when we're trying to deal with these consequences of foreign interference, we can only begin to look to ourselves as a first step in rectifying those potential threats. However, parties need to be able to take the first step.

I commend the committee for continuing this project and I hope my comments help support the recommendations for online advertising, data protections for political technology firms, and reforms to privacy and the activities of political parties.

Thank you very much.

● (1120)

The Chair: Thank you, Mr. McKelvey. Stay tuned. Those parties might show up one day.

Next up is Mr. Scott. Go ahead; you have ten minutes.

Dr. Ben Scott (Director, Policy and Advocacy, Omidyar Network): Thank you, Mr. Chair.

What brings me to sit before you today is a tale of regret. I look south at the political and democratic disaster playing out in my own country with great distress and great humility. I was among those young, idealistic, tech-savvy staffers who went to join the Obama administration in the early days after he was elected.

It was a time when we had big ideas about open data, social media, and global digital markets for speech and commerce as liberatory, as a new tool of democratic soft power, and they were—we've benefited tremendously from those forces over the last decade—but it was a double-edged sword. We were not prepared for the way that technology proved instrumental in ushering in one of the darkest chapters in American political history. We didn't do enough.

We're not alone in this. We are now seeing related phenomena across the democratic world—in Britain, Germany, Italy, France, and many other places.

The politics of resentment that we're seeing in contemporary populism mixed with the distorting power of the digital information market are a toxic brew. You have rightly pointed this out in the examination you've conducted so far, and in what we've seen in parallel examinations of this phenomenon in other legislatures.

My message to you today is a simple one: Don't wait to see how it plays out in Canada. Act right now. It will happen here too. The only question is how, and whether the consequences will be effectively mitigated in the Canadian context.

What is to be done? The first thing I want to say is, don't count on the private sector to deal with this problem. Publicly traded monopolies do not self-regulate. If we didn't know that before, we've certainly learned it over the course of the last year and a half. It brings to mind a quote that I like from my favourite chronicler of monopoly capitalism from a century ago, Upton Sinclair. He said, “It is difficult to get a man to understand something when his salary depends on his not understanding it.”

The answer here is not going to be the market; the answer is going to be government using its tools to steer the market back in the direction of the public interest. We need a kind of digital charter for democracy, one that lays out a set of principles and comes in behind it with clear policies that begin to make the changes we need to protect the integrity of our democratic public sphere.

We need to start right away, but we need to expect that this will take time. There are no single solutions to this problem. It's going to be a combination of things, none of which are sufficient by themselves, and all of which are necessary. It's going to be a messy process, because no one thing will appear to be moving the needle and making the difference that we would all like to see. However, together these things can first contain the problem, then treat the symptoms, and ultimately begin to get at the root causes of the structural problems in the market, both on the supply side and the demand side.

We begin first with security. This is the simplest and most important piece of the puzzle. The combination of cyber-attack and disinformation campaigns that we have seen unleashed on elections in several different countries is a dire threat, and we have to treat it that way. We need to increase the cybersecurity applied to our democratic institutions, including not just election administration but also political parties and campaigns. They should be treated as critical infrastructure, in my view. We also need to be much better about coordinating the research, monitoring, and exposure of disinformation campaigns that are happening with security services, with outside research entities, and with companies.

We're beginning to see a model developing in the U.S. that is worthy of examination and expansion, but let me be clear: Even if we solve the security problem, we're only eliminating a minor part of the problem. Most of the threats come from within, not from without. The most important thing in my mind about the foreign interventions we have seen across the world is that they took advantage of standard market-based tools. They were opportunistic amplifications of existing domestic political movements, and they were using tools that are perfectly well known and understood by commercial marketers across the digital world.

● (1125)

The second piece we can begin to deal with is illegal content. Again, it's not a huge part of the problem, but it's an important part. Citizens have a right to be protected from illegal content. There are now categories of content that are illegal in the off-line world; they should be illegal in the online world. These include hate speech, defamation, harassment, and incitement to violence.

All of these things can be removed on an accelerated timetable with a process that is rigorously overseen by regular judicial oversight and that has an appeals process so that we are not endangering freedom of expression when we begin to move into the space of removing illegal content. You can't cede that power to the platform companies, but we need their involvement in order to speed up the process.

Once we've dealt with the security issues and the illegal content issues, we get into the real meat of the problem: How do we mitigate the influence of disinformation campaigns that are homegrown, that begin to separate people from facts that help inform their judgments and that begin to polarize our society over time?

One thing we can do is really cultivate the research community to spend more time, energy, and money studying the problem. We simply don't know enough about how disinformation works and how the digital market works to shape political views and electoral outcomes. We need to develop ways to signal users to be wary and to be critical consumers of digital media.

Consider for a moment the average consumer who is accustomed to the traditional media environment. When you step into a news agent at an airport and look at the periodicals arrayed before you, you see the daily newspapers, and you see the political magazines and the sports, automotive, entertainment, and home and garden magazines. Depending on where you're standing, when you pick a periodical off the rack, you have a pre-set schema in your mind about what to expect.

In the digital environment, all of that is compressed into a single stream, and it looks the same. It's a Facebook newsfeed. It's a Twitter feed. It's a YouTube NextUp list of videos. In that environment, all of the signals about source credibility and quality that we once had begin to attenuate. People will tell you that they read an outrageous thing the other day and that it has really shaped their views on an important matter, whether it's climate, immigration or economic policy. You ask them where they read that, and they say they read it on Facebook—but they didn't read it on Facebook. They read it through Facebook on some other source. What was the other source? They don't remember.

We've lost the normative structure that in the old media environment allowed us as citizens to make implicit judgments about source credibility and, when we're reading digital media, to engage in critical thinking. We need to begin to find ways to understand this problem better through the research community and to begin to address it through public education and digital literacy.

As well, there are many things we can do in the market with a regulatory intervention. We can ask the companies and compel them to be much more transparent in the way they operate. This starts with political ads.

There's no reason in the world why every citizen who sees a political ad shouldn't know exactly who bought it, how much they spent, and how many people they paid to reach. Most importantly, why did I as an individual voter get that message? Is it because of my gender, my age, my income? Is it because of where I live? Is it because my characteristics are similar to those of other people they're targeting? I should be able to know that, because when I know that, it allows me to engage in a much more critical view about why that ad came to me.

To me, transparency is the simplest and easiest way to regulate the companies to move in the right direction. It's something they're voluntarily doing, but only in some countries and only when they're getting public pressure to do it. In no case has there been law laid down to mandate it. I think that's an easy first step.

There are a variety of other things that I think we ought to engage in as well. These are longer-term structural issues. They include algorithmic accountability. We need to look at how algorithms work and how they impact social welfare. We need to look at data privacy; we need to reduce the amount of data that companies collect, and we need to restrict how they use it.

Also, we need to be looking at competition policy. We need to be looking at modernizing antitrust policy to put shackles on anti-competitive practice, to restrict mergers and acquisitions, and to ease access to market entry for new kinds of services that offer alternatives to the existing models whose externalities have led to such negative outcomes.

Finally, we need to focus on the long-term task of addressing public education. We need to help people help themselves by helping them to become stronger and more insightful media consumers.

● (1130)

That includes not only digital literacy but also investments in better and more independent media. We can't expect people to steer their way away from nonsense on the Internet if there isn't a large body of quality information and journalism available to them.

I can't predict the future of where this combination of policies will go, but I do think it's the right starting point. I don't think we have a lot of time to lose. I'm encouraged and inspired by the work of this committee that government is moving in the right direction.

Thank you for your attention. I look forward to the discussion.

The Chair: Thank you, Mr. Scott.

First up is Mr. Saini, for seven minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning to everybody. Thank you very much for coming here. Your opening statements, coming from three different perspectives, have given us a lot to think about.

I would like to start with you, Mr. Owen. You talked about negative externalities. You mentioned that there have been three waves of negative externalities, one of the waves being disinformation. In one of your recent articles, you also talked about how the Overton window has been upended. Looking at that, talking about disinformation and the public space, who determines what is acceptable in the public debate, then?

Prof. Taylor Owen: I think we need to step back and look at who used to determine this. Up until the rise of the social web and the decline of legacy media that has paralleled it and is intimately related to it, we entrusted this window of acceptable discourse to a small number of legacy 20th century media institutions. This was itself a highly flawed system. It excluded a whole host of voices. It perpetuated an economic system, and arguably a political system, that benefited certain groups over others. In many ways it limited our discourse. We didn't hear from all the voices that we now have access to hearing.

When the social web emerged and new voices were given audience, we found that our debate, our public sphere, was actually much more diverse, much more dynamic, and much more informative than had been mitigated by that legacy media infrastructure. The problem now, I would argue, is that the terms of this public debate are not being defined by the value of individual voices, the societal benefit of those individual voices, or even the desired audience for those individual voices. We have a new structure that's determining what's acceptable. That structure is the filtering mechanism of platforms, deciding what we see and whether we are seen.

If we were concerned about that previous filtering model—the editors of major newspapers, the broadcasters, the small group of people who were determining what was acceptable—then we should now be concerned about the parallel filtering point, which is the algorithms and the business models that are determining what we see.

● (1135)

Mr. Raj Saini: As you know, information is sometimes conveyed by bots. There's human interaction and bot interaction. Should there be different standards, and should there be a transparency level of knowing, when we receive a message, whether this message is coming from a bot or from a human source? Should there be a standard to allow us to be able to differentiate that information in a transparent and clear way?

Prof. Taylor Owen: I believe so, yes. This has been discussed and proposed in California, where the so-called Blade Runner law would force all automated accounts to self-identify as being automated. I think in this case, transparency is the solution. There are all sorts of potential positive uses of bots and automated tools in the social ecosystem, but as consumers, we should know whether we are being targeted by one, because, importantly, this will become a much bigger issue as we engage more and more with agents and artificial intelligence-driven entities in the digital space.

Mr. Raj Saini: Okay.

Mr. Scott, I'd like to ask you a question about an article you wrote in The Atlantic about algorithms, which you mentioned in your opening remarks. As you know, certain algorithms are used to help us collect information in a much more efficient way, but it seems that algorithms now are being weaponized. One of the answers or one of the discussions by social media companies is that they should create algorithms to police the existing algorithms. Does that seem feasible to you?

Dr. Ben Scott: This reminds me of the argument that the answer to gun violence is more guns on the streets. It has a certain logic to it that you could control misbehaving algorithms with the policing algorithms, but to me the real root of the issue is not having more technology to try to patch the holes in the existing system; the real end to this problem is oversight and transparency. We need to better understand how the algorithms are working and we need to understand what the vulnerabilities are for weaponization.

In markets that have grown large and powerful and have a strong impact on the public interest, such as health and safety rules for the restaurant sector or third-party review for pharmaceuticals, we have a long history of auditing these kinds of businesses, not in order to verify that they're misbehaving intentionally but to ensure that there aren't unintended consequences to the development of products in the market. I think ultimately where we're heading is toward a system of oversight and review of algorithms that can be weaponized to ensure we don't have strong negative effects.

Mr. Raj Saini: You've said a couple of things, and it looks like I only have a minute.

One of the things you mentioned was that maybe we should limit the amount of data that is shared with social media companies. Another thing that you've said is about education, that the consumers should be more educated in being able to disseminate and differentiate between legitimate and illegitimate sources.

With the amount of information that's coming onto the Internet on a daily basis, how is it possible for somebody to be able to differentiate? What would that education piece look like? How can you educate the consumer to recognize legitimate or illegitimate information?

● (1140)

Dr. Ben Scott: It is a substantial challenge, but we had the same debate with the rise of television when we went from three or four broadcast channels to 200 channels—that the wash of information would make it impossible to differentiate credibility and quality. Over time, people developed new schema for how to sort, categorize, and judge the quality and credibility of sources on television. The same thing can happen with the Internet.

I would also emphasize that you don't need to have a Ph.D. and do a dissertation on every source that comes in to evaluate what you think about it; you need to have some quick and easy ways to evaluate how credible you find something. Those things can be taught in civics classes. They can be taught relatively broadly and in a content-neutral way so that people are simply equipped with the skills to judge when and how they ought to apply more cognitive energy to evaluate the credibility or the quality of the source.

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

Next up for seven minutes is Mr. Kent.

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

Thank you all for appearing before us today. As my colleague said, you've given us three variations of issues to consider.

Mr. McKelvey, have you shared your insight and advice with the Privacy Commissioner or the Chief Electoral Officer?

Prof. Fenwick McKelvey: I have not spoken with the Office of the Privacy Commissioner. There has been some contact with the Chief Electoral Officer. I understand there is an informal working group, but I wasn't able to attend the first meeting. Whenever I have the opportunity, I try to make myself available.

Hon. Peter Kent: You spoke of the urgency of action before the next Canadian federal election in October 2019. The Chief Electoral Officer has told the country, told the House of Commons, the government, that some of the legislation before us now is too late to enact. Do you have any suggestions that could practically be put into effect before the election to minimize or counter some of the threats you've described?

Prof. Fenwick McKelvey: I spoke about principally three things that I thought the committee hadn't heard before. The scope of this matter is something that's been quite daunting for anybody in communication studies. It's as though everything is all in one basket all at once, and what are the million different things you've studied over the past 10 years that you might pull out?

We've been trying to move fairly quickly on making recommendations. I think there has been a lot of movement on ads and ad transparency. I certainly think that more inquiry into the ad market is not necessarily hard to do. It's very evident that there's a problem there.

I think the question of other steps is one that has come up in a roundabout way. There's the question of content moderation. One of the fallacies that we have is that social media platforms are unregulated, but really we have a whole host of varying levels of rules that are more or less transparent that are filtering all content. A lot of that is for illegal content, but there have also been concerns about, for example, women's breastfeeding groups on Facebook being censored.

I think one of the steps that I and my colleagues Chris Tenove and Heidi Tworek are talking about is having a social media council, similar to a broadcasting standards council, so that you can start coordinating this kind of grey area of content moderation, which is increasingly what platforms do, and I think is largely an intractable problem. To echo Ben Scott's point, I don't think we're going to solve this thing. I think it's about developing those institutions that can maintain that.

Third, I think this code of conduct is something that really should have been done. There's reluctance by the party to do it. I'm frustrated that there haven't been any takeaways when this is something that we've been talking about for months. At some point it's not my deadline. I would hope there would be some more movement on that.

Finally, there have been discussions about Bill C-76 and privacy, and the government has stated that it's not moving forward on putting political parties under privacy law. I think that's a real shortcoming. I think it's a very easy fix, and we see it being effective in B.C.

Hon. Peter Kent: As the chair indicated with regard to the Canadian political parties, their invitations will be going out. The parties, we hope, will respond and address some of these issues.

In the case of the Cambridge Analytica-Facebook-AggregateIQ scandal, there was an awful lot of finger pointing back and forth about where the data came from and who got it. AggregateIQ said that they didn't know where the data came from, that they didn't do anything wrong, and that all they did was package it and buy advertising.

To your point about data brokers, there would also seem to be in this area a certain amount of plausible deniability about the source of the data if a party or an advertiser or anyone bought data to send a message or to buy a product or to support a political party. Do you believe there should be regulation of the data brokers in terms of how and where they acquired that information?

● (1145)

Prof. Fenwick McKelvey: I think one point is about clarifying the mandate of the Office of the Privacy Commissioner and extending their enforcement powers to potentially have more effectiveness. I don't know if it would necessarily be new regulation or just clarifying what we have already. The Office of the Privacy Commissioner has commissioned a report on data brokers. I think one of the twists that are important is that when I look at AggregateIQ and particularly the allegations that it was collecting data in Trinidad and Tobago and then moving that abroad, I think there are these questions about how we coordinate these as international players. That was my comment, that these data brokers are global. The data broker market in Canada isn't as large, according to the Office of the Privacy Commissioner, as might be the one in the United States.

I think it's in one sense realizing that our privacy laws do have some effect on that. Also it's to start thinking about how we begin to transition from collecting personal information to then thinking about these data protection laws and about how we're putting those combinations together, and how much transparency there is in that. I think there is clear need for that.

Hon. Peter Kent: Very briefly, because time is precious here, to Mr. Owen and to Mr. Scott, what are your thoughts on the reality that the digital universe is without borders? When the GDPR, the General Data Protection Regulation, was brought in in Europe, we saw that quite a number of large American news organizations began blocking access from Europe because they weren't sure whether or not they would actually be breaking these new laws in those jurisdictions.

What are your thoughts on this current situation in which the GDPR has one set of very stringent regulations but the rest of the world is without?

Prof. Taylor Owen: I would just say that I think we're seeing the emergence of three competing regulatory regimes: a European regulatory regime that's in many ways articulated through GDPR but also through other provisions; an American regime, now largely unregulated in structure, that supports the dominance of current American-based platform companies; and a Chinese governance model that is building and providing tools that provide a much higher degree of surveillance and monitoring capacity than any other tools available. I think there's an opportunity for a fourth. There's a demand globally for something different from those three regimes, but if Canada is not going to provide it, then I think we have to pick one of those regimes. This idea that we can sit between Europe and America on this issue is unsustainable.

The Chair: Thanks.

We'll move on to Mr. Masse.

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

That's an interesting point to pick up on. One of my biggest concerns in this, and I propose a digital bill of rights, is that we seem to be seeking, or at least some do, to put the genie back in the bottle.

I can tell you that as a New Democrat I've had many reporters come to me and tell me from their paper that they won't cover me because their editorial will not cover an NDP member. I've been doing this for 15 years federally, and for five years on municipal council prior to that. We have streams, layers, screens in the mainstream media. It is exciting for the Internet to be used as a different vehicle to actually reach people through different messaging, and it has had an impact.

I had a bill on motor vehicle owners' right to repair in the automotive aftermarket. It got limited coverage because the advertisers had a very lucrative relationship with the automotive companies. This is a provision that was done in the United States for aftermarket repairs. Over in Canada, you were directly competing in messaging against those who have a financial interest in the distribution of commercials and advertising, which is quite lucrative.

I am intrigued, though, by the disclosure of transparency that's being proposed, and maybe I could get some further comment on that. I will leave this open to all of the members. We could see it as similar to drug coverage. When advertisers ask you to prescribe yourself a drug on TV or whatever, there's a disclaimer. We know that *SNL* and others have done famous comedy sketches where they run the side effects for nausea. Is that a model or is it a potential element?

I'll conclude with this. The use of telecommunications in the airwaves and the airspace is a public infrastructure that we lease out. It is ours and we own it like the land we have. We pay for the devices, the fees, and the services to actually get this information to us and our families. They're often infected or contaminated by others, who attack it through malware and other types of phishing and other things, so I believe there's a high responsibility on those who are perpetrating this type of information. How we would enhance the transparency from the perspective I have is that we should at least have some rights on this issue because we've created the system for this distribution of information.

● (1150)

Dr. Ben Scott: If I could, maybe I'll jump in on that point.

I think transparency is the clearest set of recommendations that we have, and a number of ideas have been floated.

I published a paper yesterday that I could draw your attention to. It's called "Digital Deceit II". It is the second in the series. The first was on ad tech; this one is on policy recommendations.

There's a very specific recommendation for ad transparency in that paper. Essentially what it says is that when you get an ad on Facebook or Twitter or YouTube, when you put your finger over that ad if it's on your phone, or you hover your cursor over that ad if it's on your desktop, it ought to pop up a little box that tells you a lot more information about that ad: who bought the ad; how much they paid for it; how many people have seen it besides you; and, most importantly, why you got that ad—what the demographic features were that were chosen by the advertiser to make that ad come to you. If you got that ad because the advertiser somehow has your email address or your phone number, they should have to say that too. When I have all that information, I realize, "Wow—I'm going to view this piece of information a lot more critically."

Our study shows us that a lot of people don't even realize the difference between an ad and organic content, non-paid content.

I think those ads should have a big red box around them so you know they're ads. "I'm going to put my finger over that. I want to see more about why I got that."

This is directly analogous to how we treat broadcast advertising or pharmaceutical advertising. We have a public interest responsibility for transparency, and we provide for that in the law. There's no reason we can't do that in digital. The companies could do this tomorrow if they wanted to.

The other piece is that all the politicalized ads that come up on Facebook or Twitter or Google ought to be in a database that is publicly accessible. With a lot of political ads, there are a thousand different versions of that ad, and they're microtargeted at small groups of people. Sometimes there are contradictory messages and they're just hoping that no one will notice they're advertising two different things to two different groups. You could never do that on television—you'd get busted in a second—but you can do it in Facebook with no problem.

The Trump campaign was a master at this. We need that database to be accessible to journalists and researchers through a very simple API so that everybody can get access to that data and look at it and understand how political propaganda is working. It's not that it's all illegitimate, only that we ought to know what's happening and how people are trying to influence our views.

Mr. Brian Masse: Does anybody else have a comment?

Prof. Taylor Owen: I agree completely with both elements of that. That really is the first and easiest step in the lead-up to in the next election.

Mr. Brian Masse: Go ahead, Mr. McKelvey.

Prof. Fenwick McKelvey: I do want to caution that.... I think transparency is quite important. I think there also is a need to start talking about the limits of where you can advertise and how you can advertise. This is why I think the bill of rights is kind of interesting. You were starting to stipulate what can and can't be done and shifting some of the responsibility off consumers, who I think are in a taxed information environment, and putting it on the responsibility of companies.

I think one of the telling lessons for me was that both Facebook and Google have exited from providing advertisements for cryptocurrencies, and Google in particular has stopped providing ads for opioid treatment centres because they are too difficult to regulate.

I think what we need to say is that these ad markets are already being policed in ways and that we need to have more transparency about how they work. I think it's not simply about transparency for the user, but also greater accountability about how these ads are being sold and managed.

● (1155)

The Chair: You have about 10 seconds.

Mr. Brian Masse: Quickly, can government set an example by going first with putting the standards on themselves and then bringing the private sector in right after that?

Prof. Taylor Owen: Absolutely.

Dr. Ben Scott: Yes.

Prof. Fenwick McKelvey: Yes.

The Chair: Wow, three answers in three seconds. That's pretty good.

Next up, for seven minutes, is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

Thanks for presenting today.

In June, we tabled an interim report with specific recommendations, and I want to make sure we're on the same page. You would all agree with strengthening the powers of the Office of the Privacy Commissioner. Is that fair to say?

Prof. Fenwick McKelvey: Yes.

Dr. Ben Scott: Yes.

Prof. Taylor Owen: Yes.

Mr. Nathaniel Erskine-Smith: You've all spoken today about better regulation of political activities with respect to privacy. I want to drill down on that so that when we get to a final report, we maybe have some more specific recommendations.

When we talk about elections and ad transparency, both Mr. Owen and Mr. Scott, you've delineated in different papers an exact way of looking at this. There's the searchable database on Facebook, where a political actor like myself would post content. That content should be searchable, presumably, if I'm sponsoring it.

Would that make sense?

Dr. Ben Scott: That database already exists if you're an American Facebook user.

Mr. Nathaniel Erskine-Smith: Yes, although I understood from speaking to some folks in the States that it was not so easily searchable and requirements should be imposed on its searchability.

Dr. Ben Scott: I was going there next; you beat me to it.

When Facebook, Google, and Twitter announced they were going to do ad transparency databases, they said you're going to see all the ads that are run during a political cycle and you're going to have data about every single one of them: who bought the ad, how much they spent, and some information about targeting, although they've reneged a little on that. It was all going to be searchable and there was going to be API access so that researchers and journalists could literally download the entire data set and study it themselves.

That last piece has not been done. The searchability and the research capability of that data set are not up to the standard we need. I don't believe the companies are going to get there on their own, nor should we expect them to. These are businesses. They don't want to reduce the amount of commercial advertising revenue coming in the front door. Their responsibility isn't to protect the public interest. That's ours.

If we want that standard to be in the market, we're going to have to put it in the law.

Mr. Nathaniel Erskine-Smith: When it comes to subjecting political activities to a privacy regime, it's one of our recommendations, but when we did have Christopher Wylie here, he indicated there ought to be a difference between how we treat political activities and how we treat profit-seeking enterprise, because of course the pursuit of democracy is different from the pursuit of dollars. Do you see there would be a differentiation between the stringency of that privacy regime, or should we apply the same regime to both enterprises?

Dr. Ben Scott: I've wrestled with this question myself. I think you can differentiate them. I think there is a logic to differentiation to suggest that we have a standard for political advertising that is different from selling soap or bicycles, just as we do in broadcast ads.

It becomes more challenging when you start asking what a political ad is. It's interesting to see how the three big platform companies have defined political ads in what they put in their databases and what they apply their voluntary regulation to.

Twitter says an ad is only a political ad if it mentions a political candidate or a party. That's the Google standard as well. Facebook says a political ad is anything that mentions an issue of public importance, and they list about 20, including everything from climate to gun control to immigration. To me that's a much more honest presentation of what a political ad looks like. I think it's a mistake to limit your terms too narrowly, because people will just go around you and use different things as proxies, but once you begin to define it more broadly, the grey zone between what's political and what's non-political becomes more challenging to define.

I think it's like night and day: 95% of the time we can agree whether it's night or whether it's day. We'll adjudicate those 5% of cases that have legitimate opinions on both sides. I think they can be divided. I think that's the right starting point. If we find that a company can't distinguish between the two, fine; you can just make the same high bar for everything.

● (1200)

Prof. Taylor Owen: Very briefly, I think Ben Scott and I agree on most of this range of policy responses here, but on this one there might be a bit of distance between us. In the long run I'm not sure we can make that distinction between political and non-political ads in a viable and sustainable way.

Ultimately, whether it's for commercial or political activity, both are seeking to influence our behaviour. Why wouldn't we, as either consumers in a consumer protection realm or voters in an election integrity realm, be allowed to know how our behaviour is being microtargeted using incredibly sophisticated systems to target and nudge our behaviour? I see different baselines for both, but the easier solution is to make it all transparent.

Mr. Nathaniel Erskine-Smith: We talked about advertising transparency. Mr. McKelvey, you talked about collection and use and more stringent requirements on the collection and use of personal information and subjecting political activities of political parties to stronger requirements perhaps. If I knock on a door and I speak to someone and they say they're really interested in climate change and then I target an ad to that individual among other individuals who are all concerned about climate change, do we have a problem with that?

Prof. Fenwick McKelvey: I think, in principle, getting to your question, political parties can easily fit within our existing privacy law. If you're collecting information about their views at the door, then it seems to me—not being a privacy lawyer—that there's an informed consent. You're asking them for their views, and that's something you're collecting and they know you're collecting it. Then you're using it.

I think it comes into a question, which I think is a question writ large in our data in this kind of combination of surveillance and targeting: When do we know, and when are we informed that information you're collecting is going to be used for targeting purposes?

The point that I'm trying to make is that I'm not convinced that all this targeting is super-effective. If you're a political party and you want to target people about climate change, why do you need to link that to the voter whose door you're knocking on in the first place? I think that there are ways you can abide by the privacy law and still be able to conduct relatively the same type of business.

It gets into whether you're sending a specific targeted email to that person who's talking about climate change. You know, maybe that might be restrained in some way.

Mr. Nathaniel Erskine-Smith: Do I have much time?

The Chair: You have one second. Unless you can be as quick as Mr. Masse, it's—

Mr. Nathaniel Erskine-Smith: Maybe you'll get back to me.

The Chair: Okay.

We have five minutes for Monsieur Gourde.

[*Translation*]

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

I thank the witnesses for being here this morning.

From your discussions, we all understand that the current digital world is evolving, that it is changing and transforming. The various digital platforms provide us with a whole new landscape of information, but also of misinformation, which is unfortunate.

We have been seeing over the past two or three years just how much fake news is taking over all digital platforms. We are wondering whether Canadians will drop out at some point because no one can any longer be sure how accurate the information provided is. Is it real or fake? That is a current issue in the United States, where news is provided one day, refuted the next, but again presented as real the day after.

The public is confused by these new media, which have unfortunately taken over part of the traditional media's market. I think that traditional media were more ethical because they spent more time on their research before providing information to the public.

There is also the issue of advertising on those platforms. I think that new media care little about the accuracy of the advertising they air. Who do you think should be responsible for the veracity of advertising proposed by both the private sector and political parties? You can each answer in turn.

● (1205)

[*English*]

Prof. Fenwick McKelvey: If I understand correctly, the credibility of advertising is a real issue. That's where I've noted companies like Facebook and Google exiting from certain ad markets or restricting ad options for certain keywords, such as “cryptocurrency” and “opioid addiction treatment centre”.

I think it's very important to recognize that this is a clear limitation when you have some of these algorithmic markets being constituted. It's that they suffer at times from being able to recognize quality or credible information.

I think that is one of the ubiquitous problems that we have. To operate at scale, information triage has kind of taken on a market-like approach. I think that it has often failed in delivering high-quality ads, or at least with opioid addiction treatment centres, ads that aren't from scammers or dubious treatment centres.

I think that's an important finding. It's important to recognize that there are real challenges in how algorithmic recommendation takes place and whether that functions effectively in being able to discern what's good and bad information, to use those terms super-loosely.

Mr. Jacques Gourde: Go ahead.

The Chair: Hold on, Mr. Owen. We're not getting....

Okay, go ahead.

Prof. Taylor Owen: I have a quick point on trust of information. I think it's pretty clear that trustworthy information that is known by a large number of citizens is critical to a democracy. We have to have some baseline of trustworthy information on which we are making democratic decisions about our collective well-being and governance. This is critical to a democracy, and that is being eroded by the system.

If we take that as our baseline, then I think we need to look at how we create more trust and more reliable information in the ecosystem we now have in our digital public sphere. Certainly advertising credibility is a part of it, ad transparency, but a big piece is the amount of journalism that is being produced in our society about our society and is holding power accountable within our society, and that is in steep and precipitous decline in Canada.

There are a host of other regulatory changes or points of governance engagement that could help make that more robust. There are easy things, such as changing the Income Tax Act to allow for charitable funding of news. In the U.S., the most robust sector in the journalism space, particularly the accountability journalism space, is non-profit news. This is almost non-existent in Canada because of our charitable funding law.

I think there is a whole host of things we could do, at the very least, to build up that backstop of reliable journalism in this space as well.

Prof. Fenwick McKelvey: I would add to that also, thinking about public broadcasting. I think that one of the ways that we're seeing this issue is that we think about information subsidies, or what's subsidizing the production of information, and I think there is a whole host of new information subsidies. This is when you talk about native content or sponsored content, as well as propaganda campaigns. That's really where, to me, it's also looking to public broadcasting as another important source and realizing that part of the integrity of our democracy is funding public broadcasting.

The Chair: Thank you, Monsieur Gourde.

Next up, for five minutes, is Monsieur Picard.

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

In order for the government to regulate, we have to identify the real problem or problems. Let's go back to the basics of the question at stake, the breach of personal information. What is the problem with Facebook and Cambridge Analytica? Is it the fact that someone was intelligent enough to draw conclusions about the behaviour of people based on public information provided by subscribers, or because they did it without our knowing it?

Dr. Ben Scott: To me, the problem is both. I'll answer—

The Chair: I'll start with Mr. McKelvey and then go to Mr. Scott.

Dr. Ben Scott: Chair, I have something I want to say on this.

The Chair: Sorry, Mr. Scott. We had Mr. McKelvey first, and then we'll go to you.

Dr. Ben Scott: I apologize.

Prof. Fenwick McKelvey: I was just going to say that what is clear is that what's been exposed—and I think what Facebook has also admitted before this committee—is that they have been entrusted with a lot of personal information and data and they have not been discerning about who has access to that personal information. I'm quite skeptical of whether Cambridge Analytica was effective, and I'm not particularly convinced about the psychometrics as some sort of revolutionary new hypodermic needle, but I am thinking that it is very clear that if you're collecting large amounts of data, there is an obligation under the privacy law to make sure that you're controlling the flow and who gets access to it.

I think it's been very clear that this has been one of the key issues here, the kinds of data-sharing arrangements that have taken place in social media.

● (1210)

Mr. Michel Picard: I'll get back to Mr. Scott.

Is it access, or is it knowing what they would do with the data?

Prof. Fenwick McKelvey: Well, part of the concern is that there was access provided without clear oversight on how they were going to use that data. This is one of the things that's creating a challenge for academic research too. Facebook and many other social media platforms have tightened up their APIs and their data access. That was often done without much transparency—and that's what Facebook has admitted—about how that data was going to be used, so I think it's twofold: it's basically knowing who has access to it and also making sure they're subject to accountability about what they're doing with the data.

Mr. Michel Picard: Mr. Scott, would you comment?

Dr. Ben Scott: I want to point to two interesting provisions in Europe's General Data Protection Regulation. We are not sure yet how they are going to be adjudicated and applied in the market.

One of those provisions says the user should have more control over the consent they give to different kinds of information. Right now, when I sign the Facebook privacy agreement, it's all or nothing. I either agree to whatever is in that 80-page document or I don't use the service. The GDPR says you can't do that anymore. You have to give people meaningful choices when it comes to controlling their own data, especially sensitive data such as that which shapes political views.

I think there's a key question about giving consumers more ability to control what data is collected and how it's used. The German antitrust regulator, interestingly, has launched an inquiry into Facebook. It says that the market power a company like Facebook has over a segment of social networking is so strong that effectively their privacy agreement is a coercion—that it's all or nothing. There's no way for the consumer either to know or to have an incentive to know what's in there, because to say “no” is to abandon the service altogether and not get access to something that two billion on the people on the planet are using.

To me, this points to the fundamental problem. Exactly as Professor McKelvey says, you need to know what they're collecting, and not only do you need to know how they're using it, but you need to have a say in how they're using it. That's what I think is consumer control over the application of my data. That's the key piece that I think we're wrestling with in privacy policy, but it has implications in competition policies as well, because market power plays a big role.

Mr. Michel Picard: Thank you.

Mr. Owen, you said in your opening speech that this impacts democracy and that our electoral system is at risk. It sounds good in political speech, but in reality, what is the problem with it? People say whatever they want about any candidate. Is the problem that our system has been hacked, or can people make up their own minds in cross-checking information they get?

Prof. Taylor Owen: Well, I don't think it's been hacked. I think it's just that the marketplace for our information is structured very differently than it used to be. In that old model, we had all sorts of ways of and mechanisms for limiting and regulating speech during elections, for foreign money going into the media market, for forced disclosures from broadcasters of who's paying for what ad during an election.... These things are the ways that we regulated speech in order to protect our public sphere during the time of an election, noting that this was a particular moment in our society when quality information was important.

Those regulations and laws aren't very applicable in this new ecosystem. The question is, do we think they need to apply? Do these same principles need to apply in this new ecosystem? I would argue that they do, but that the regulations need to look different because the structure of that ecosystem is different.

The Chair: Thank you, Mr. Picard.

Next up for five minutes is Mr. Kent.

Hon. Peter Kent: Thank you very much, Chair.

Before Christopher Wylie became a whistleblower, in pitching the ability to affect election or referenda outcome, he made a statement saying that essentially “we can trigger the underlying dispositional motivators that drive each psychographic audience”.

Dr. McKelvey, I know that you have said you're a bit skeptical of the psychographic microtargeting concept, but we understand from Chris Vickery and others that, rather than the half-dozen or dozen data points that many advertisers use to target responses when they observe the browser history of an individual, Cambridge Analytica, in this case—and ultimately AggregateIQ in Victoria—was working with as many as 500 data points on individuals to exploit their vulnerabilities, such as their sexual preferences, perhaps, or their fears or anxieties.

Do you completely disregard this concept of psychographic microtargeting? Otherwise, do you believe that there is a line that should be drawn on how much data can be used in targeting advertising?

● (1215)

Prof. Fenwick McKelvey: Part of my research is historical. In the 1980s, the Claritas Corporation was using geodemographics and psycho-demographics. In one sense, I think that one of two things can be true. Psycho-demographics can either be something relatively new—the point when you encounter it in the literature is the 1980s—or it's been a myth that the advertising industry has been trying to sell their products with for 30 years. I'm of the latter category.

I think it's a good way of selling their categories. I think that's where I actually have.... My opinion is that I'm not convinced it works. I'm not convinced that you need to collect all this information. I'm not convinced that psycho-demographics is really that effective. In particular, I also think that when you're looking at campaigns with limited resources, they're not writing ad copy for 500 different categories.

Now, there's a certain threat that AI might change that, but I think that for right now, if you tend to think this doesn't work and this probably isn't great, why are we enabling all this data to be collected? If you look at the literature, it says that three or four different variables are really good predictors of actual voter intent. I mean, beyond me, I think it's the question of why we are enabling all this other data collection if there's limited benefit to it.

I'm not against the idea that it might work; I'm skeptical of its overstated claims.

Hon. Peter Kent: Go ahead, Mr. Owen.

Prof. Taylor Owen: I don't think we should be making regulatory change based on whether the claims of one particular company to do one particular thing using one particular database at one particular moment were effective or not.

I think principles, such as the consent and knowability that Ben just mentioned, are protections against the possibility of that kind of misuse. If we consent regularly to the use, sharing and amalgamation of our personal data—if we have the right to that consent—and if we have the right to know how that data is being used, whether it's for psychographic profiling, for an AI-driven microtargeting campaign, or for whatever reason, that protects us and inoculates us against the potential risk of these technologies in the future, not how they were used in one moment of time by one group.

Dr. Ben Scott: To me, the takeaway from the Cambridge Analytica episode is not that Cambridge Analytica had some special sauce of psychographic manipulation; it's that they were basically using the same tools of microtargeting that Facebook makes available to everybody. They overstated that dramatically in their marketing materials, but I think microtargeting to find audiences that are responsive to particular messages is effective. Facebook makes $40 billion a year in revenue for a reason. I don't think you have to imagine a splashy new way of doing that called Cambridge Analytica to make that meaningful. I think data-driven targeting is the name of the game in advertising today, and we ought to be regulating at the root, rather than in fancy branches.

Hon. Peter Kent: In the absence of regulation, and in the North American context or Canadian context, there's recognition that the individual owns their own personal data. You've all spoken to the need for education of the users.

When I speak to high school classes or seniors' groups, they take the cautions about participating in polls, playing games online, or guarding their browsing history almost with a grain of salt. Would any of you recommend that the social media companies set aside large amounts of money, not to provide the education service themselves, but for third parties or independent groups to better educate social media users from the early school grades right through life?

Prof. Taylor Owen: I think digital literacy campaigns are incredibly important, but only if done at scale. Who funds that scale? That could be incentivized to the platform companies to put money into that. There's a real government role there, too, for a large-scale digital literacy campaign, not just to separate blatantly true from blatantly false information. That dichotomy is very rarely presented to a user. Rather, users need to understand the system in which they are participating—why they're receiving what they're receiving, what data is being used about them and how that shapes the content they're getting. If we embed those kinds of conversations in our digital literacy campaigns at scale, then we can make some progress.

● (1220)

The Chair: Thank you, Mr. Kent.

Next up for five minutes is Madam Fortier.

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): Frank is taking my turn.

The Chair: Mr. Baylis, go ahead.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Start the clock now.

I want to come back to the concept of news, information, and the data. It's a simple question we've always asked ourselves. Who's selling you your news? We've always bought news. If we take away the Internet and throw it away, we've got, say, Fox and CNN on TV. To your point, Mr. Scott, when you talk about your list of magazines, I turn on the TV and if I know I want to hear a certain story about a certain president, I'll watch CNN. If I want to hear the same story told a totally different way, I'll watch Fox. That has nothing to do with the Internet, but I'm making a choice as a consumer to buy my news. Now you're saying I can buy it on the Internet with my eyeballs.

A lot of people give it to me for free if I just watch their ads or spend time with them. Other times they'll say that if I want to get, say, The New York Times or The Wall Street Journal, I've got to pay for a subscription.

Using that as a background, another concept we worry about is filtering. Before, we had filters. They were the editor, the publisher, and ultimately the owner of a newspaper. All kinds of people like me —politicians—would have to go and, quite frankly, suck up to these guys so they'd write something nice about us. That's the reality of it. They've actually been weakened.

Great, positive things have come through with the Internet. Twitter has allowed us to speak directly to our people, unfiltered. As you said, Mr. Scott, there are also nefarious things that can come out of this.

You've spoken about transparency. Is transparency the issue? We are always going to buy our news. We are always going to go to a source that can tell us what we want to hear. In that sense of looking at news, written news, looking at TV, and now looking at the Internet, what is the one thing we should be doing there?

Go ahead, Mr. Scott. I'll start with you.

Dr. Ben Scott: I think transparency is only one piece of the puzzle.

I'm a big believer in the decentralization of the communications system. It's a good thing that we have more voices, more journalists, more reporting. The fact that it is no longer a viable business is a big problem, and we need to address that as a systematic issue in the market.

There is a second piece to this. Consumers are at the beginning of a long process of learning how to consume information on the Internet, in the same way that it took us decades to figure out how to consume information on broadcast channels. In the early days of radio, you could see a similar debate playing out. People said, “Wow, everybody is being misled by this new thing called broadcasting. It's completely different from newspapers. You hear it over the radio and it seems true, and people just take it.” That was considered incredibly alarming.

Now, as you have clearly pointed out, we all know how to differentiate what we want on broadcast. That will come eventually on digital media. The trick here is that it's push versus pull. Instead of going on TV and selecting CNN or Fox, Facebook is being pushed at me.

There are 10,000 different news items that are sitting in my Facebook account that Facebook could choose to show me, but I'm only going to see about 5% of them. Facebook decides which 5% I'm going to see. It decides that based on what it thinks I want, not what I choose.

That may be a business that I'm willing to sign up for, but I need to understand much more about why that happens, and why I'm getting what Facebook has decided I should get. Right now, we don't have that. That's why people are so vulnerable to misinformation.

Mr. Frank Baylis: What's the one thing you would do to give us that?

Dr. Ben Scott: I think it's transparency in the algorithm, an increase in quality journalism, and digital literacy. Without all three of them, you're not going to move the needle substantially.

Prof. Taylor Owen: Can I make a point on the quality journalism aspect of this question?

Mr. Frank Baylis: Go ahead, Mr. Owen.

Prof. Taylor Owen: The reason we've seen the precipitous decline of the financial viability of the journalism sector as it was previously constructed is that the advertising revenue that it once depended on is gone. That is the reality. If that had led to a fertile digital ecosystem of vibrant digital start-ups, doing better journalism than their legacy institutions were, we wouldn't have a problem. That is not what has happened, at least in Canada, yet.

If that's what we want to create and enable, then we need to look at policies that can help enable that emerging journalism production. Maybe we're okay with the amount of journalism being done now, as it's produced in our democracy, but I argue we shouldn't be. For example, there are around 100 newspapers left in Canada. Their total revenue is now lower than the revenue of the CBC. I personally don't think that's a healthy ecosystem. There are a host of journalism-related policies we could talk about to help enable this new ecosystem.

● (1225)

The Chair: Go ahead, Mr. Masse, for three minutes.

We do have some time afterwards if there are further questions to be asked of the group. We have them until 1 p.m. Let me know if you have a question.

Mr. Brian Masse: What would be the quick fix, if there is one, going into the next election that we have coming up? Time is running out.

What should be the consequences for those who break whatever rules we have? Should they be highly punitive, or should it be a carrot-and-stick approach?

Dr. Ben Scott: I can jump in on that. There are four things you can do right now before the end of the year to prepare for 2019.

One, aggressive political ad transparency should be applied by law on all of the platform companies.

Two, increase the amount of money and coordination of those who are monitoring and exposing foreign intervention directed at misinformation campaigns.

Third, elevate quickly a process for removing illegal content, with all of the proper caveats about free expression, so that we don't have to suffer from things that shouldn't be out there in the first place.

Fourth, start talking to young voters in the classroom. My kids are in this wonderful program in Canada called Student Vote. In it they do mock elections and learn about political parties and the political system. We should have a digital literacy component in that curriculum.

Mr. Brian Masse: Would anyone else like to comment?

Prof. Taylor Owen: I agree with those four.

Prof. Fenwick McKelvey: Yes. I think enforcement mechanism is quick. I think one of the challenges is how you develop tools during the election to combat some of these things. This is where I think a code of conduct would be important, because, if you think of parties, if all of a sudden one party is benefiting from foreign interference, how do all parties respond? I think that's a tough question that talks about the conduct of our elections.

I think this kind of enforcement mechanism—I think a lot of the stuff is illegal—is about trying to bring greater transparency to this, whether this is content moderation, as has been discussed, or whether it talks about ad markets.

Prof. Taylor Owen: On enforcement, there is a reason that GDPR sets the penalties at global revenue, not localized revenue, because if you don't do that, there's very little incentive for structural change. I think that's a cue on where we need to go on the penalty side.

The Chair: You have 30 seconds.

Mr. Brian Masse: Go ahead, please, Mr. McKelvey.

Prof. Fenwick McKelvey: I also want to add widening our scope of online advertising. We've been mostly talking about programmatic advertising. This is when you loop in bots, sponsored content, and influencer marketing, which is all this grey area of promotional content that's taking place on social media. We have to move forward in recognizing the scope and ubiquity of the advertising we see today.

Mr. Brian Masse: Thank you, Mr. Chair.

The Chair: Thanks, everyone.

We have more time, so does anybody have any further questions?

We will start with Mr. Erskine-Smith for five minutes.

Mr. Nathaniel Erskine-Smith: Just to pick up where we left off on transparency, I think it makes it sense that political advertising would not be treated particularly differently than other advertising. Give no answer now, because I want to get to something else, but do think about collection and use and how political parties or political activities should perhaps be subject to different rules or the same rules. If you have further thoughts, it would be great if you could submit them to the committee.

I want to get to the policing of content on the Internet, because both Mr. Owen and Mr. Scott have touched on this in their writing. You have suggested that these big platforms have the capacity and resources to do the work.

How do we set a rule that requires certain organizations to police content and not others, if smaller organizations don't have the capacity and resources?

● (1230)

Dr. Ben Scott: We have a couple of different models to look at. I will profile the German model and tell you where I think it went right and where it went wrong.

The Germans set a bar, I think, of a million domestic subscribers to the service, which basically meant three companies—Google, Facebook, and Twitter—and they said, "You have 24 hours to remove illegal content from the moment you get notified that it's there".

The problem with that was that they put all the burden on the companies. They gave all the decision-making authority to the companies about what was and wasn't illegal, and they had no appeals process.

The benefit they got from that was the resources and the technical ability of the companies to rapidly find not only the content that drew a complaint, but all content like that and all copies of that content all across the network and to quickly bring it down, much as they do for copyright violations, much as they do for other forms of fraud and illegal content. Counterterrorism functions the same way.

In my view, the problem is that we need more regular order judicial review. The prosecutors who would normally have brought a case like that through the usual court procedure ought to be involved in the oversight so that when the algorithm comes back and says these are the thousand cases of this piece of hate speech we see on the network, there is either a common review of that content to ensure it's meeting a public interest standard of free expression, legal/illegal, or it goes into an appeals process and goes through regular order judicial review.

Mr. Nathaniel Erskine-Smith: Why not flip that on its side? If you have ever had a parking ticket in Toronto, there's an administrative system that makes you subject to a $50 fine unless you explain yourself. If I post something hateful on the Internet, part of the problem with our system right now is that the response is the Criminal Code, right? There's no good ability to penalize either me, who has published the hateful content, and there's certainly no imposition upon the platform at the moment to take it down or pay a penalty if they don't.

Why not tax the big players and have a public administrative system that has a quick takedown system in the first instance, rather than putting the obligation on these companies to police it themselves?

Dr. Ben Scott: In theory, on paper, there's no reason you couldn't do it that way. In practice, the administration of that technical system is non-trivial and requires access to those companies' infrastructures, which they are not likely to want to provide.

I think it's certainly something that should be on the table for discussion about a long-term solution, but in the short term, if what we need, for example, between now and October 2019 is the ability to remove intentional hate speech and illegal content off the Internet in a hurry, we're going to have to find a more straightforward mechanism.

Mr. Nathaniel Erskine-Smith: In the short term, that probably means the platforms themselves taking it down.

In terms of regulating platforms, the U.K. recently suggested in their recommendations that there should be a category of platforms that are subject to regulation. If you look at the CRTC right now, they regulate publishers and broadcasters, but we don't regulate these platforms that claim not to be either of those things.

Is the body that should regulate these platforms, whatever threshold we set, the CRTC? Is it the Privacy Commissioner? Where should this reside?

Prof. Taylor Owen: I think Professor McKelvey might be best positioned to answer this one.

Prof. Fenwick McKelvey: I'm currently working with Chris Tenove and Heidi Tworek on a report about content moderation. First off is that there is no one jurisdiction that's going to regulate these platforms. I think they are multi-jurisdictional and I think that's actually something that's not a problem. We have that with broadcasting and telecommunications.

In terms of the Privacy Commissioner and the CRTC with regard to the ways platforms function, I think they do at times function specifically as broadcasters as well as, I think, a specific new category that deals with this content moderation problem. I think it's important to recognize that they fit into existing jurisdictions and need to be held accountable with regard to the ways in which their activities fit within those, but then I think there's this content moderation question that we really have not given any serious legislative attention to. What we have is kind of a piecemeal amalgam of hate speech laws and revenge porn laws.

One of the things I, along with my co-authors, am recommending is a social media standards council or a content moderation standards council similar to a broadcasting standards council. If you look at what the broadcasting standards council looks like, it's very parallel to what has been called for and what we need in content moderation, with an appeals process, transparency, and disclosure. I think the concern and the push-back I have to give back are that's it's more industry self-regulation. I think there is a criticism there, but I think that's an important first step that would actually start convening around this particular activity of content moderation, which we have not recognized well before the law.

● (1235)

Mr. Nathaniel Erskine-Smith: But we impose—

The Chair: Hold on. You're out of time.

Mr. Nathaniel Erskine-Smith: I'm out of time. No worries.

The Chair: Mr. Baylis, you have five minutes.

Hold on. There are more in the queue before Ms. Vandenbeld. She just got added to the end.

Mr. Frank Baylis: I'll give her my spot because I've already spoken. I'll switch spaces with her. If I don't make it, that's fine, Chair. Thank you.

The Chair: Okay.

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

Actually, I wanted to pick up on that particular thought. It's one thing to moderate content when there is actual hate speech or something that is outright misogynistic. What you've been discussing today is more about the algorithms and the fact that the toxic platform actually prioritizes the kind of speech that might not reach the threshold of hate speech but is still racist or has underlying sexist messaging.

The difference, for instance, with television is that when you put on a commercial, everybody sees the same commercial. Obviously it has to be moderated to be what most people would want to see and consider to be acceptable versus, for instance, if somebody did something that might have underlying misogynistic undertones and they click on it and it says "The reason you got this is that you are a white male between the ages of 20 and 25 and you just broke up with your girlfriend."

If they knew that, then that would allow that person to think twice and say, "Why am I getting this?"

Is this what we're talking about here? I'm asking because there are two different things. There's actual hate speech and then there's the way in which all of these messages are being targeted at individuals, and that's a lot harder to regulate.

Prof. Fenwick McKelvey: The thing is that there's a distinction between hate speech, which is captured under the Criminal Code, and what I think is an increasingly growing concern, which is harmful speech. We don't want to conflate the two. As a male who has grown up online, and having talked to my female counterparts, I think there's concern about the amount of aggression. I think this is also particularly true now for female politicians. Just think about the amount of vitriol being spewed. I think there is some way of dealing with that, which is different from dealing with hate speech, both in terms of concern and in terms of tactics.

That's part of that content moderation, and that already happens on social media platforms. Social media platforms are already making decisions about what content is accessible. Instagram producers online are already struggling with what parts of their body they can expose or not expose based on the content moderation of that platform.

The specific point about this is about recommendation. This is how platforms make recommendations about what content you see. This is often described as a filter bubble, whereby they're filtering your content. I think there is less concern about the filter bubble than there is about the fact that if you look at YouTube, it optimizes for engagement. If you look at Facebook, it's for meaningful social interactions.

It's those particular kinds of logic that are recommending content that might have some, to use Taylor Owen's words, negative externalities. We need to have more transparency about the consequences of those recommendations, and in particular about some of the ways there might be some red lines about what content can be recommended. I think a standards council could be one of the ways. I also think that when you get into the enforcement issue and you're trying to shut down hate speech quickly, that's another point at which there might be intervention.

Ms. Anita Vandenbeld: Mr. Owen, would you comment?

Prof. Taylor Owen: More broadly on the content moderation issue, there's clearly a broad spectrum of potential harmful speech and a broad range of ways to address different problems along that spectrum—hate speech, child pornography, and criminal activity on one end of the extreme, and maybe just political views we don't agree with on the other end. We'll engage different things in different spaces, and that's fine.

The other important point here is that there is national context to the way we regulate speech, and that is okay. We know what the alternative default is. If we're not imposing those national guidelines, regulations, and incentives on speech, the default is the interpretation of the terms of use of a global company. Twitter has terms of use different from Facebook's, and Google/YouTube has terms of use different from the other two. We know, for example, that Twitter has a very free-speech-leaning application of its terms of use. Up until recently, almost anything was allowed. Twitter was incentivizing engagement and activity over the limiting of speech. That was a corporate decision, and that has caught different consequences in different national environments.

In Canada, we have criminalized hate speech. When we did that, there was a lot of push-back from free-speech advocates in the United States, who said Canada was limiting speech too much, but we made that decision as a democracy ourselves and then built an infrastructure to apply it.

The questions for us now in Canada—which are different from the questions for Germans, for instance, who have a different application of hate speech for various historical reasons—are how we are going to apply our current hate speech standards onto platforms, and whether we are going to extend those hate speech provisions to other kinds of content that we now think have negative costs in society beyond those original provisions. Those are two separate questions, I think.

● (1240)

The Chair: Thank you, Mr. Owen.

Next up, we have Brian Masse for five minutes.

Mr. Brian Masse: Thank you, Mr. Chair.

One of the presentations I found interesting was with regard to the regulations around bots and artificial intelligence, although we didn't get too much into it. Would it be worthwhile for Canada to create a type of regulatory environment for how bots can be used for advertising and content distribution? I'm just throwing that out in terms of what we would do here. Also, should we be looking at including this as part of some of our trade agreements?

I worked on the anti-spam legislation. There are serious problems with that legislation, as you know, but the volume of information and its use, and the consequences from malware and other things, are quite economically significant, let alone irritating.

Maybe we can start with Mr. McKelvey. Do you have any comments about bots and whether there should be domestic rules and perhaps international rules with regard to that activity?

Prof. Fenwick McKelvey: I think Dr. Owen summed it up nicely. There are transparency requirements. It's about trying to make sure that when there is bot activity, we know it's a bot, and that there is disclosure around it.

I've actually thought it comparable to the voter contact registry, the VCR. The issues of the VCR and whether that can be done for bots.... I don't think it should be done on a per-bot basis, but if companies do large-scale social media amplification, that could be subject to it.

In many ways, it's performing this kind of placement cost. If you're paying a bot to amplify your message, there are ways to refine it. It's about counting it as advertisement and disclosing it as such. That would actually go a long way. I think because it targets that specific type of bot, we have a problem, which is what I would describe, along with Elizabeth Dubois, as an amplification bot. This is a bot that is adding more credibility to something and kind of "Astroturfing". If we count this as advertising, that would be an important step toward normalizing it within this advertising system.

Prof. Taylor Owen: I would briefly add that the bot issue is in many ways the tip of the iceberg of a much bigger conversation that you alluded to, which is around the governance of AI. This issue we're talking about today, about information in our democracy, is embedded in a much larger debate about how we should be governing automated elements in our society, whether they be individual agents, advertisers, medical providers, or whoever they might be.

We need to have a conversation about consent and data access, two systems that use our data, and about knowing how that data is used. That will require a broader conversation beyond the Canadian context. In many ways, it's becoming, and emerging as, a global regulatory conversation.

It's part of this conversation we're having.

● (1245)

Prof. Fenwick McKelvey: I also want to say that the federal government is currently investigating right now the ways it's governing itself in AI. The Treasury Board is looking into impact assessments for AI. As it's rolling out, how is AI being deployed in the federal service? There's a review process being put in place.

I think this is important evidence of how the government could be a leader in AI governance. I think it also requires awareness that the rollout is done transparently and that these kinds of concerns about the potential political use of these technologies are factored in. I think there's really important work taking place presently.

Mr. Brian Masse: Thank you, Mr. Chair.

The Chair: Thank you.

Next up, for five minutes, is Monsieur Picard.

Mr. Michel Picard: Thank you.

We have a journalist who is very serious in his work and who surely provides credibility to the newspaper he works for. Here we are, though, with someone who cannot talk about my NDP colleague because someone else decided to prevent his readers from knowing what's going on in his riding. When I look at news on TV, and when I look at the different U.S. channels especially, they seem to be very serious channels, but depending on which channel I look at, the United States seems like two different countries.

You referred to trust a few minutes ago, and to the source of information that you can have access to. What were you referring to, anticipating that trust is a possible notion?

Prof. Taylor Owen: Trust is a difficult concept in relationship to journalism. I might trust Fox News and you might trust MSNBC, and we both have high degrees of trust in the journalism we're consuming, so I'm not sure that's the core metric on an individual level.

On a societal level, I think we can talk about how much trustworthy and accurate information is in our public sphere, is circulating, and whether that's enough. I think that's the point on which we need to engage in this. It's not whether each individual trusts the particular news source they're getting their content from, but whether as a society we have a collective body of reliable information in our democracy.

Mr. Michel Picard: Go ahead, sir.

Prof. Fenwick McKelvey: It's very strange for me, as someone who teaches communication and media studies. I have had long-standing criticism, I think shared by many people, about the gatekeeping effects of the media and the decline of the for-profit media. It's not something that anybody comes here holding in high regard.

I think the challenge is that in one sense, you were looking at these gatekeepers as people that you knew. That's kind of the way the system worked. What we're now facing is that we just don't know how that system works. We don't know how the influencers work. There's strategic power in the fact that there's inequitable information there.

One thing that needs to be said is that there are a variety of solutions that need to be put forward. I think in Canada we've kind of said that we have a more proactive cultural policy and that we can function as information subsidies for the public good. When we're talking about trust in the media, this is where public broadcasting has been shown to be really effective in raising the bar for any kind of misinformation or disinformation campaign, making it more difficult to do, and in also putting good information out there. It's really clear to me that the public benefit of public broadcasting is something that is ever more true, that is unique, and it should continue to be part of the robust solution Canada takes to these concerns.

Mr. Michel Picard: Unfortunately, Facebook is not owned by Radio-Canada, so there's no public medium like Radio-Canada broadcasting on Facebook, the Internet, or whatever media you use. Therefore, with any source available, when you rely on your Facebook page, you get tons and tons of awkward information. Government cannot regulate laziness. If I don't cross-check my information, as Mr. Scott said, I'm going to read my Facebook and think the world is the way Facebook describes it to me.

It's all a matter of interests. For me, the important thing is to be able to know what interests are behind the information and therefore have the availability to verify this information with other sources and make up my own mind. Would that be the limit of my intervention as a government, and of course the responsibility of any reader?

Prof. Fenwick McKelvey: I would joke that the CBC should buy Reddit, in part because I think we had about a 10-year gap when we really weren't thinking about what public broadcasting means in an era of social media. I still think we have in many ways a really limited sense of what the potential of social media could be, and I think there's room for imagination and thinking more broadly.

I also think that one of the benefits as we're talking about the sharing of information is that if you give away the information for free as a public good, you are creating and fuelling these platforms with good information and seeding it.

We can talk about the concentration of the social networking space or the advertising space, but I think if we're just talking about access to information, public broadcasting plays an important role there.

● (1250)

Mr. Michel Picard: Mr. Scott, Mr. Owen, would you comment?

Dr. Ben Scott: Our goal here is not the elimination of bias or sensationalism or nonsense in the media system. They will always be there and the media have always been all those things. Our goal here is to contain those things such that most of the people most of the time are shaping their political views based on a fact-based, rational view of their society.

How do we get that done? It's changed. When there are major shifts in the dominant form of information distribution, a new set of norms has to emerge about how you get to that result of most of the people most of the time. The way we did that in the broadcast area was through a heavy investment in public media, and we relied on journalistic standards in the newspaper market. Now we have a tremendous disruption, the biggest disruption in public information since the printing press, and we are going about the task of figuring out how we establish the right norms by controlling the supply side: by using privacy policy to limit filter bubbles, by using competition policy to ensure there's space in the market for other kinds of providers, and by investing in digitization of public media.

We're also working on the demand side, helping consumers understand that the passive consumption—

The Chair: I hate to cut you off, Mr. Scott. We've got to move on to the next questioners.

We have two questions to close.

We'll go to Mr. Saini and then Mr. Kent, and then we're done. My apologies.

Mr. Raj Saini: Mr. McKelvey, in something you wrote a while back, you had three topics: discoverability, trending, and advertising.

I want to focus on discoverability, because discoverability for me is doing something indirectly that you can do directly with advertising. You have an issue, and the users or the platform companies highlight that, and then the algorithms push that to the top of the list. Then if someone without any prior knowledge wants to research a topic, a candidate, or a particular position and they go to the Internet and they google that name, that negative piece or the most salacious piece will appear.

You've written about that. What can be done to prevent it? I think that can be done indirectly. If you have advertising, you're directly advertising, but this is an indirect way of also getting out a position. The existing algorithms seem more insidious than the advertising component.

Prof. Fenwick McKelvey: I think the discoverability of things is a really important thread, so thank you for picking that up. To me, discoverability means what shows up when you search for something. I would point to some of the research I've done in the Algorithmic Media Observatory. We looked at discoverability of political content during the Ontario election to see how the recommender system was working. The CBC also did a similar study and reported on it.

I think that the way you're feeling with that is, first, to look at what counts. What are these systems ranking information for? I think we're still trying to find intentions, so this is talking about engagement or meaningful social interactions. I think those are things to be attended to. An explicit judgment is being made, and I think it's for the government to put forward good recommendations or good cultural policies for other forms of discoverability as a government norm.

I think it's also trying to recognize...I point to the report of data in society, which has just come out and talks about influencer networks. I think it's important to say that discoverability is a system that works, but we don't necessarily know how. It's clear that through coordination you can influence these discoverability systems, and I think that's one point that points to research. Particularly if people are being paid to influence or change discoverability, I think that could count as a form of advertising.

The Chair: Thank you.

Last up, we have Mr. Kent.

Hon. Peter Kent: Thank you very much, Chair.

Thank you all for the various remedies you suggested for the surveillance-of-capitalism side of what we've been talking about today, but human nature being what it is, people are still enthusiastically joining and participating in the relationship-enabling aspect of social media, which is after all the origin of social media today.

I'd like to come back to the foreign intervention in the electoral process that we talked about a little earlier. I think it was Dr. Scott who gave the example of the Russian-confected Beyoncé fan site, Trojan Horse time bomb. How do you prevent that sort of confected site leading up to an election, which is detonated just at decision-making time?

● (1255)

Dr. Ben Scott: I think it's very difficult to guard against that kind of attack.

Here's where the state of the art is now. Essentially it's a collaboration among security services, outside researchers, and companies to try to detect in advance the coordinated activity of disinformation operators. There are signals in the network if you know how to look for them, and they're developing tools and they're doing what they call red teaming, which is to put yourself in the perspective of a malignant actor who might try that Beyoncé trick. How would you go about doing that? If you can do it, what are the ways that could be countered?

If we can think of it in an imaginative red team exercise, you can be sure that our adversaries are thinking of it as well, and you build prophylactic defences against those things that you can imagine doing. It's a very Cold War war-gaming exercise, and that's what's going on right now in the cybersecurity space.

You're not going to be able to defend against all of these things. You're only going to be able to contain a certain percentage, so the second piece of this is resilience. You need to have a plan in place to react very rapidly when that time bomb is triggered and suddenly something happens that you weren't expecting. You need to be able to react fast to bring it down and to educate the public who were contacted by that account that they have been engaged by either an automated account with malignant intent or a foreign-operated influence campaign. Those rapid response techniques are also things we ought to be developing.

Hon. Peter Kent: Thank you.

The Chair: Thank you, everybody, for attending today and providing us with a lot of food for thought.

Thanks to the committee for coming today. It's a good first meeting of the session. Thanks again, and we'll talk soon. Have a good day.

The meeting is adjourned.