HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 120 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 16, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 16, 2018

● (1105)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): We're going to start the meeting now. I'm Nathaniel Erskine-Smith. I'm filling in for Mr. Zimmer, who is our usual chair. I'll ask some questions, but I'll leave it to my Liberal colleagues to ask most of them.

We'll start with 10-minute statements from each witness here today and then move to rounds of questions.

We'll begin with Ms. Wardle from Harvard University.

Dr. Claire Wardle (Harvard University, As an Individual): Thank you very much for your invitation to appear today. My apologies for not being able to attend in person.

I am Dr. Claire Wardle. I'm a research fellow at the Shorenstein Center on Media, Politics and Public Policy at Harvard's Kennedy School.

I'm also the executive chair of First Draft. We are a non-profit dedicated to tackling the challenges associated with trust and truth in a digital age. We were founded three years ago specifically to help journalists learn how to verify content on the social web, specifically images and videos. That remains my research speciality.

In 2016, First Draft began focusing on mapping and researching the information ecosystem. We designed, developed and managed collaborative journalism projects in the U.S. with ProPublica, and then in 2017 ran projects in France, the U.K. and Germany during their elections. This year we're currently running significant projects in the U.S. around the mid-terms and the elections in Brazil, so we have a lot of on-the-ground experience of information disorder in multiple contexts.

I'm a stickler for definitions and have spent a good amount of time working on developing typologies, frameworks and glossaries. Last October, I co-authored a report with Hossein Derakhshan, a Canadian, which we entitled “Information Disorder”, a term we coined to describe the many varieties of problematic content, behaviours and practices we see in our information ecosystem.

In the report, we differentiated between misinformation, which is false content shared without any intention to cause harm; disinformation, which is false content shared deliberately to cause harm; and, malinformation, which is a term we coined to describe genuine content shared deliberately to cause harm. An example of that would be leaked emails, revenge porn or an image that recirculates during a hurricane but is from a previous natural disaster, our point being that the term “fake news” is not helpful and that in fact a lot of this content is not fake at all. It's how it's used that's problematic.

The report also underlined the need for us to recognize the emotional relationships we have with information. Journalists, researchers and policy-makers tend to assume a rational relationship. Too often we argue that if only there were more quality content we'd be okay, but humans seek out, consume, share and connect around emotions. Social media algorithms reflect this. We engage with content that makes us laugh, cry, angry or feel superior. That engagement means more people see the content and it moves along the path of virality.

Agents of disinformation understand that. They use our emotional susceptibilities to make us vulnerable. They write emotion-ridden headlines and link them to emotional images, knowing that it is these human responses that drive our information ecosystem now.

As a side note, in our election projects we use the tool CrowdTangle, which now has been acquired by Facebook, to search for potentially misleading or false posts. One of the best techniques we have is filtering our search results by Facebook's angry face reaction emoji. It is the best predictor for finding the content that we're looking for.

I have three challenges that I want to stress in this opening statement.

First, we need to understand how visuals work as vehicles for disinformation. Our brains are far more trusting of images, and it takes considerably less cognitive effort to analyze an image compared to a text article. Images also don't require a click-through. They sit already open on our feeds and, in most situations, on our smart phones, which we have a particularly intimate relationship with.

Second, we have an embarrassingly small body of empirical research on information disorder. Much of what we know has been carried out under experimental conditions with undergraduate students, and mostly U.S. undergraduate students. The challenges we face are significant and there's a rush to do something right now, but it's an incredibly dangerous situation when we have so little empirical evidence to base any particular interventions on. In order to study the impact of information disorder in a way such that we can really further our knowledge, we need access to data that only the technology companies have.

Third, the connection between disinformation and ad targeting is the most worrying aspect of the current landscape. While disinformation itself at the aggregate level might not seem persuasive or influential, targeting people based on their demographic profile, previous Internet browsing history and social graph could have the potential to do real damage, particularly in countries that have first-past-the-post electoral systems with a high number of close-fought constituencies. But again, I can't stress enough that we need more research. We simply just don't know.

At this stage, however, I would like to focus specifically on disinformation connected to election integrity. This is a type of information disorder that the technology companies are prepared to take action around. Just yesterday, we saw Facebook announce that around the U.S. mid-terms, they will take down, not just de-rank, disinformation connected to election integrity.

If disinformation is designed to suppress the vote, they can take action, whereas in other forms of information disorder, without external context, they are less willing to take action in a way that actually right now is the right thing.

In 2016 in the U.S., visual posts were micro-targeted to minority communities, suggesting they could stay at home to vote for Hillary Clinton via SMS, giving a short code. Of course, this was not possible. As a minimum, we need to prioritize these types of posts. At a time when the whole spectrum is so complex, that's the type of post we should be taking action on.

In terms of other types of promoted posts that can be microtargeted, there is a clear need for more action; however, the challenge of definitions returns. If any type of policy or even regulation applies simply to ads that mention a candidate or party name, we would be missing the engine of any disinformation campaign, which is messages designed to aggravate existing cleavages in society around ethnicity, religion, race, sexuality, gender and class, as well as specific social issues, whether that's abortion, gun control or tax cuts, for example.

When a candidate, party, activist or foreign disinformation agent can test thousands of versions of a particular message against endless slices of the population, based on the available data on them, the landscape of our elections looks very different very quickly. The marketing tools are designed for toothpaste manufacturers wanting to sell more tubes, or even for organizations like the UNHCR. I used to do that type of microtargeting when I was there, to reach people who were more likely to support refugees. When those mechanisms have been weaponized, what do we do? There is no easy solution to this challenge. Disinformation agents are using these companies exactly as they were designed to be used.

If you haven't read it already, I recommend you read a report just published by the U.K.'s leading fact-checking organization, Full Fact. They lay out their recommendations for online political advertising, calling for a central, open database of political ads, including their content, targeting, reach and spend. They stress that this database needs to be in machine-readable formats, and that it needs to be provided in real time.

The question remains how to define a political ad and whether we should try to publicly define it. Doing so allows agents of disinformation to find other ways to effectively disseminate their messages.

I look forward to taking your questions on what is an incredibly complex situation.

Thank you.

● (1110)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much, Dr. Wardle.

Next up are Mr. Black and Mr. Tseng. Both are lawyers at McMillan LLP.

Mr. Ryan Black (Partner, Co-Chair of Information Technology Group, McMillan LLP, As an Individual): Thanks very much.

Good morning, members of the standing committee and fellow witnesses.

I am Ryan Black, partner and co-chair of information technology at McMillan LLP, a national law firm. With me is Pablo Tseng, my colleague in our business and intellectual property groups. We're practising lawyers in British Columbia, and we're honoured to be here today by video conference at the request of the standing committee.

Mr. Pablo Jorge Tseng (Associate, McMillan LLP, As an Individual): A few months ago, Ryan and I wrote an article entitled "What Can The Law Do About 'Deepfake'?" The article provides an overview of the causes of action that may be taken against those who create and propagate deepfake material across the Internet, including across social media platforms.

Some of the causes of action include those related to defamation, violation of privacy, appropriation of personality, and the Criminal Code. However, the article did not focus on how deepfakes may influence elections, or how we as a nation can limit the effects of such videos on the outcome of an election.

We hope to use our time here today to further our thoughts on this very important topic. Our opening statement will be structured as follows: one, provide an overview of some other legal mechanisms that are available to combat deepfake videos in an election context; two, provide an overview of potential torts that are not yet recognized in Canada but have the potential to be; and three, discuss whether deepfakes really are the problem or just another example of a greater underlying problem in society.

Mr. Ryan Black: From the outset, we want to ensure that the appropriate focus is placed on the roles that users, platforms and bad actors themselves play in propagating social media content. Well-intended platforms can and will be misused, and deepfake videos will certainly be a tool used in that malfeasance.

The true bad actor, though, is the person creating the false media for the purpose of propagating it through psychological manipulation. As Dr. Wardle alluded to, the data is valuable, and platforms generally want technology to be used properly. They assist law enforcement agencies with upholding relevant law, and develop policies intended to uphold the election's integrity. They also allow for the correction of misinformation and the sourcing of information.

A recent example in Canada is Facebook's Canadian election integrity policy, which is posted on the Internet.

I'll turn it over to Pablo to discuss the legal remedies relevant to today's discussion.

Mr. Pablo Jorge Tseng: Focusing on elections, we wish to highlight here that Parliament is forward-thinking in the fact that in 2014, they introduced a provision to the Elections Act directed to the impersonation of certain kinds of people in the election process. While such provisions are not specifically targeted at deepfake videos, such videos may very well fall within the scope of this section.

In addition, there have been examples in our Canadian case law where social media platforms have been compelled through what courts call Norwich orders to assist in the investigation of a crime committed on that social media platform. For example, a social media platform may be compelled by a court to reveal the identities of anonymous users utilizing the services of that social media platform. That is to say that legal mechanisms already exist and, in our experience, law-abiding third parties subject to such orders generally comply with the terms thereof.

There is also room for our courts to expand on common law torts and for governments to codify new ones.

In general, laws exist in common law and statute form. It is important not to lose sight of the fact that governments have the ability to create law; that is, governments are free to come up with laws and pass them into force. Such laws will be upheld, assuming that they comply with certain criteria. Even if they do not necessarily comply with those criteria, there are certain override provisions that are available.

An example of codification of torts is British Columbia's Privacy Act, which essentially writes out in statute what the cause of action of appropriation of personality is.

Today we are flagging two other torts for discussion: unjust enrichment and the tort of false light.

With regard to unjust enrichment, such tort has generally been upheld in cases involving economic loss suffered by the claimant. However, it is reasonable to argue that the concept of losses should be expanded to cover other forms of losses that may not be quantifiable in dollars and cents.

Regarding the tort of false light, such tort exists in some states of the United States. Canada, however, does not recognize this tort just yet. However, the impact of deepfake videos may cause Canadian courts to rethink their position about the tort of false light. Even if this tort of false light does not exist in common law, it is very well within the power of the provincial government to enact the tort into statutory code, thereby creating its existence via statutory form.

● (1115)

Mr. Ryan Black: In our article, we explore copyright tort and even Criminal Code actions as potential yet sometimes imperfect remedies. We note that deepfake, impressive and game-changing no doubt, is likely overkill from manipulating the public. One certainly would not need complex computer algorithms to fake a video of the sort routinely serving as evidence or newsworthy.

Think back really to any security footage you have ever seen in a news incident. It's hardly impressive fidelity. It's often grainy or poorly angled, and usually only vaguely resembles the individuals in question.

While deepfake might convincingly place a face or characteristics into a video, simply using angles, poor lighting, film grain, or other techniques can get the job done. In fact, we've seen recent examples of speech synthesis seeming more human-like by actually interjecting faults such as ums, ahs, or other pauses.

For an alternative example, a recent viral video purportedly showed a female law student pouring bleach onto men's crotches on the Russian subway to prevent them from the micro aggression of manspreading, or men sitting with legs too splayed widely apart. This video triggered an expected positive and negative reaction across the political spectrum. Reports later emerged that the video was staged with the specific intent to promote a backlash against feminism and further social division in western countries. No AI technology was needed to fake the video, just some paid actors and a hot button issue that pits people against each other. While political, it certainly didn't target Canadian elections in any conceivably actual manner.

Deepfake videos do not present a unique problem, but instead another aspect of a very old problem worthy of consideration certainly, but we do have two main concerns about any judicial or legislative response to deepfake videos.

The first is overspecification or overreaction. We've long lived with the threat that deepfake poses for video in the realm of photography. I'm no visual effects wizard, but when I was an articling student at my law firm more than a decade ago, as part of our tradition of roasting partners at our holiday parties, I very convincingly manipulated a photograph of the rapper Eminem replacing his face with one of our senior lawyers. Most knew it was a joke, but one person did ask me how I got the partner to pose. Thankfully, he did not feel that his reputation was greatly harmed and I survived unscathed.

Yes, there will come a time when clear video is no longer sacred, and an AI-assisted representative of a person's likeness will be falsified and convincingly newsworthy. We've seen academic examples of this already, so legislators can and should ensure that existing remedies allow the state and victims to pursue malicious deepfake videos.

There are a number of remedies already available, a lot which will be discussed in our article, but in the future of digitally manipulable video, the difference between a computer simulation and the filming of an actual physical person may be a matter of content creator preference, so it may, of course, be appropriate to review legal remedies, criminal offences, and legislation to ensure that simulations are just as actionable as physical imaging.

Our second concern is that any court or government action may not focus on the breadth of responsibility by burdening or attacking the wrong target. By pursuing a civil remedy through courts, particularly over the borderless Internet, it will often be a heavy burden to place on the victim of a deepfake, whether it's a woman victimized by deepfake revenge pornography, or a politician victimized by deepfake controversy. It's a laborious, slow and expensive process. Governments should not solely leave remedy entirely to the realm of victim-pursued legislation or litigation.

Canada does have experience in intervening in Internet action to varying degrees of success. Our privacy laws and spam laws have protected Canadians, and sometimes burdened platforms, but in the cybersecurity race among malicious actors, platforms and users, we can't lose sight of two key facts.

First, intermediaries, networks, social media providers, and media outlets will always be attacked by malicious actors just as a bank or a house will always be the target of thieves. These platforms are, and it should not be forgotten, also victims of malicious falsehood spread through them just as much as those whose information is stolen or identities falsified.

Second, as Dr. Wardle alluded to, the continued susceptibility of individuals to fall victim to fraud, fake news, or cyber-attack speaks to the fact that humans are inherently not always rational actors. More than artificial intelligence, it is the all too human intelligence with its confirmation bias, pattern-seeking heuristics, and other cognitive shortfalls and distortions that will perpetuate the spread of misinformation.

For those reasons, perhaps even more than rules or laws that ineffectively target anonymous or extraterritorial bad actors, or unduly burden legitimate actors at Canadian borders, in our view governments' response must dedicate sufficient resources to education, digital and news literacy and skeptical thinking.

Thanks very much for having us.

● (1120)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much to you both.

Next up, from San Francisco, we have Tristan Harris, co-founder and executive director of the Center for Humane Technology.

Mr. Tristan Harris (Co-Founder and Executive Director, Center for Humane Technology): Thank you, Mr. Chair.

I am Tristan Harris. It's a pleasure to be with you today. My background was originally as a Google design ethicist, and before that I was a technology entrepreneur. I had a start-up company that was acquired by Google.

I want to mirror many of the comments that your other guests have made, but I also want to bring the perspective of how these products are designed in the first place. My friends in college started Instagram. Many of my friends worked at the early technology companies, and they actually have a similar basis.

What I want to avoid today is getting into the problem of playing whack-a-mole. There are literally trillions of pieces of content, bad actors, different kinds of misinformation, and deepfakes out there. These all present this kind of whack-a-mole game where we're going to constantly search for these things, and we're not going to be able to find them.

What I'd like to do today is offer a diagnosis that is really just my opinion about the centre of the problem, which is that we have to basically recognize the limits of human thinking and action. E.O. Wilson, the great sociobiologist, said that the real problem of humanity is that we have paleolithic emotions, medieval institutions and god-like technology. This basically describes the situation we are in.

Technology is overwriting the limits of the human animal. We have a limited ability to hold a certain amount of information in our head at the same time. We have a limited ability to discern the truth. We rely on shortcuts like what other people are saying is true, or the fact that a person who I trust said that thing is true. We have a limited ability to discern what we believe to be truthful using our own eyes, ears and senses. If I can no longer trust my own eyes, ears and senses, then what can I trust in the realm of deepfakes?

Rather than getting distracted by hurricane Cambridge Analytica and hurricane addiction and hurricane deepfakes, what we really need to do is ask what the generator function is for all these hurricanes. The generator function is basically a misalignment of how technology is designed to not accommodate, almost like the ergonomic view of a human animal.

Just like ergonomics, where a pair of scissors can be in my hands and I can use it a few times, it will get the job done. However, if it's not geometrically aligned with the way the muscles work, it actually starts to stress the system. If it's highly geometrically misaligned, it causes enormous stress and can break the system.

Much like that, the human mind and our ability to make sense of the world and our emotions have a kind of ergonomic capacity. We have a situation where hundreds of millions of teenagers, for example, wake up in the morning, and the first thing they do when they turn off their alarm is turn their phone over. They are shown evidence of photo after photo after photo of their friends having fun without them. This is a totally new experience for 100 million teenage human animals who are waking up in the morning every day.

This is ergonomically breaking our capacity for getting an honest view of how much our friends are having fun. It's sort of a distortion. However, it's a distortion that starts to bend and break our normal notions and our normal social construction of reality. That's what's happening in each different dimension.

If you take a step back, the scale of influence that we're talking about is unique. This is a new form of psychological influence. Oftentimes what is brought up in this conversation is, “Well, we've always had media. We've always had propaganda. We've always had moral panic about how children use technology. We've always had moral panic about media.” What is distinctly new here? I want to offer four distinct new things that are unprecedented and new about this situation.

The first is the embeddedness and the scale. We have 2.2 billion human animals who are jacked into Facebook. That's about the number of followers of Christianity. We have 1.9 billion humans who are jacked into YouTube. That's about the number of followers of Islam. The average person checks his or her phone 80 times a day. Those are Apple's numbers, and they are conservative. Other numbers say that it's 150 times a day. From the moment people wake up in the morning and turn off their alarms to the moment they set their alarms and go to sleep, basically all these people are jacked in. The second you turn your phone over, thoughts start streaming into your mind that include, “I'm late for this meeting”, or “My friends are having fun without me.” All of these thoughts are generated by screens, and it's a form of psychological influence.

The first thing that's new here is the scale and the embeddedness, because unlike other forms of media, by checking these things all the time, they have really embedded themselves in our lives. They're much more like prosthetics than they are like devices that we use. That's the first characteristic.

● (1125)

The second characteristic that's different and new about this form of media propagandic issue is the social construction of reality. Other forms of media, television, and radio did not give you a view of what each of your friends' lives were like or what other people around you believed. You had advertising that showed you a theoretical couple walking on a theoretical beach in Mexico, but not your exact friends walking on that specific beach and the highlight reels of all these other people's lives. The ability to socially construct reality, especially the way we socially construct truth, because we look at what a lot of other people are retweeting, is another new feature of this form of psychological manipulation.

The third feature that's different is the aspect of artificial intelligence. These systems are increasingly designed to use AI to predict the perfect thing that will work on a person. They calculate the perfect thing to show you next. When you finish that YouTube video, and there's that autoplay countdown five, four, three, two, one, you just activated a supercomputer pointed at your brain. That supercomputer knows a lot more information about how your brain works than you do because it's seen two billion other human animals who have been watching this video before. It knows the perfect thing that got them to watch the next video was X, so it's going to show another video just like X to this other human animal. That's a new level of asymmetry, the self-optimizing AI systems.

The fourth new distinct thing here is personalization. These channels are personalized. Unlike forms of TV, radio or propaganda in the past, we can actually provide two billion *Truman Shows* or two billion personalized forms of manipulation.

My background in coming to these questions is that I studied at the Persuasive Technology Lab at Stanford, which taught engineering students essentially how to apply everything we knew about the fields of persuasion, Edward Bernays, clicker training for dogs, the way slot machines and casinos are designed, to basically figure out how you would use persuasion in technology if you wanted to influence people's attitudes, beliefs and behaviours. This was not a nefarious lab. The idea was could we use this for good? Could you help people go out and get the exercise they wanted, etc.?

Ultimately, in the last class at the Persuasive Technology Lab at Stanford, someone imagined the use case of, what if in the future you had a perfect profile of what would manipulate the unique features, the unique vulnerabilities, of the human being sitting in front of you. For example, the person may respond well to calls from authority, that the Canadian government's summoning the person would be particularly persuasive to his or her specific mind because the person really falls for authority, names like Harvard or the Canadian government, or is really susceptible to the fact that all of his or her friends or a certain pocket of friends really believed something. By knowing people's specific vulnerabilities, you could tune persuasive messages in the future to perfectly manipulate the person sitting in front of you.

This was done in the last class of my persuasive technology class, done by one of the groups. It was on the future of the ethics of persuasive technology, and it horrified me. That hypothetical experiment is basically what we live inside of every single day. It's also what was more popularly packaged up at Cambridge Analytica where, by having the unique personality characteristics of the person who you're influencing, you could perfectly target political messaging.

If you zoom out, it's really all about the same thing, which is that the human mind, the human animal is fundamentally vulnerable, and there are limits to our capacity. We have a choice. We either redesign and realign the way the technology works to accommodate the limits of human sense making and human choice making or we do not.

As a former magician who can tell you that these limits are definitely real, what I hope to accomplish in the meeting today is we have to bring technology back inside those limits. That's what we work on with our non-profit group, the Center for Humane Technology.

● (1130)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much, Mr. Harris.

As our last witness, we have Ms. Krause, researcher and writer.

Ms. Vivian Krause (Researcher and Writer, As an Individual): Good morning, Mr. Chairman. It's a privilege to appear before your committee. Thank you for the opportunity.

My name is Vivian Krause. I'm a Canadian writer and I have done extensive research on the funding of environmental and elections activism. My understanding is I have been asked to speak to you today on the topic of elections integrity and specifically about issues related to social media.

Based on my research, Mr. Chairman, it is clear to me that the integrity of our 2015 federal election was compromised by outside interests. Furthermore, our federal election was compromised because the charities directorate at the CRA is failing to enforce the Income Tax Act with regard to the law that all charities must operate for purposes that are exclusively charitable.

I'll get to the CRA in a minute, but first I'd like to speak briefly about the non-Canadian organizations that intervened in the 2015 election and why. As evidence, Mr. Chairman, I would ask your committee to please take a look at the 2015 annual report of an American organization called the Online Progressive Engagement Network, which goes by the acronym OPEN. This is an organization based in Oakland, California. I have provided a copy to the clerk. In the annual report the executive director of OPEN writes that his organization based in California ended the year 2015 with “a Canadian campaign that moved the needle during the national election, contributing greatly to the ousting of the Conservative Harper government.”

Who is OPEN, and how did it involve itself on the 2015 federal election? OPEN is a project of the strategic incubation program of an organization called the Citizen Engagement Laboratory, CEL. The Citizen Engagement Laboratory has referred to itself as the people behind the people. It says on its website that it is dedicated to providing best-in-class technology, finance, operations, fundraising and strategic support.

What does OPEN do exactly? According to OPEN, it provides its member organizations with financial management, protocols, and what it calls surge capacity in the early days of their development. OPEN helps “insights, expertise and collaboration flow seamlessly” across borders, adding that this helps new organizations to “launch and thrive in record time”.

Indeed, that is precisely what Leadnow did in the 2015 federal election. As part of his job description for OPEN, the executive director says he was employed to “advise organizations on every stage of the campaign arc: from big picture strategy to messaging to picking the hot moments”.

OPEN is funded, as least partially, by the Rockefeller Brothers Fund based in New York. Tax returns and other documents, which I have also provided to the clerk, state that since 2013 the Rockefeller Brothers Fund has paid at least $257,000 to OPEN. In its literature, OPEN describes itself as a B2B organization with “a very low public profile”. It says this is intentional as the political implications of an international association can be sensitive in some of the countries in which it works. In its Facebook profile, the executive director of OPEN says of himself that he can see the Golden Gate from one house—in other words, from San Francisco—and the Washington monument from the other—in other words, the White House—and he adds that he spent a lot of time interloping in the affairs of foreign nations.

What did OPEN do exactly in the 2015 federal election? OPEN helped to launch Leadnow, a Vancouver-based organization. We know this because OPEN's executive director tweeted about how he came to Canada in 2012, stayed at a farmhouse near Toronto and worked with Leadnow. Other documents also refer to OPEN's role in launching and guiding Leadnow.

We know for sure that Leadnow was involved with OPEN because there's a photo of Leadnow staff in New York attending an OPEN meeting with the Rockefeller Brothers Fund in 2012. Another photo of Leadnow is at an OPEN meeting in Cambridge, England, and there is a photo of Leadnow staff in Australia in January 2016, shortly after the federal election, winning an award from OPEN, an American organization, for helping to defeat the Conservative Party of Canada.

Leadnow claims credit for helping to defeat 26 Conservative incumbents. That's a stretch, I would guess, but in a few ridings I think it stands to reason that Leadnow may have had an impact on the vote.

● (1135)

For example, in Winnipeg's Elmwood—Transcona riding, where Leadnow had full-time staff, the Conservative incumbent lost by only 61 votes. Leadnow has presented itself as a thoroughly Canadian youth-led organization, the brainchild of two university students, but as we now know, that is not the whole story.

I think it is important to note that this Rockefeller-backed effort to topple the Canadian government did not emerge out of thin air. This effort to influence Canada's federal election was part and parcel of another Rockefeller-funded campaign called the tar sands campaign, which began in 2008, 10 years ago. Indeed, the tar sands campaign itself has also taken credit in writing for helping to defeat the federal government in 2015.

For many years, the strategy of the tar sands campaign was not entirely clear, but now it is. Now the strategy of the tar sands campaign is plenty clear, because the individual who wrote the original strategy and has been leading the campaign for more than a decade has written, “From the very beginning, the campaign strategy was to land-lock the tar sands so their crude could not reach the international market where it could fetch a high price per barrel.”

Now, turning to the CRA, I'll be brief. As an example of what I regret to say I think is a failure on the part of the charities directorate to enforce the Income Tax Act, I referred the committee to three charities. These are the DI Foundation, the Salal Foundation, and Tides Canada Foundation. As I see it, the DI Foundation and the Salal Foundation are shell charities that are used to Canadianize funds and put distance between Tides Canada Foundation and the Dogwood initiative. The DI Foundation, a registered charity, has done absolutely nothing but channel funds from Tides Canada Foundation to the Dogwood initiative, which is one of the most politically active organizations in our country.

In the 2015 federal election, the Dogwood initiative was a registered third party, and it reported, for example, that it received $19,000 from Google. The Dogwood initiative is also one of the main organizations in the tar sands campaign, as it received more than $1 million from the American Tides Foundation in San Francisco. One of its largest funders, in fact, I believe its single largest funder, is Google.

According to U.S. tax returns for 2016, Google paid Tides $69 million. The Tides Foundation in turn is one of the key intermediary organizations in the tar sands campaign, and has made more than 400 payments by cheques and wire transfers to organizations involved in the campaign to landlock Canadian crude and keep it out of international markets.

Mr. Chairman, in conclusion, I think it's important to note that the interference in the 2015 federal election was done with a purpose. It was done as part of a campaign to landlock one of our most important national exports. I hope that my remarks have given you a glimpse of some of the players that were involved, the magnitude of the resources at their disposal, and perhaps also some actionable insights about what your committee could do to better protect the integrity of our elections in the future.

Thank you very much.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much for that presentation.

We're going to go to seven-minute rounds. We have about an hour and 20 minutes, so we'll get one full round in, and then we'll have some time for additional questions.

The first seven minutes go to Mr. Baylis.

● (1140)

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

I'll start with you, Ms. Wardle. What I'd like to do first of all is put some nomenclature around all the different things that are going on. You've used “misinformation,” “disinformation,” and “malinformation”. Mr. Black and Mr. Tseng have used “deepfakes”, deepfake videos. Do they fit into one of your three categories?

Dr. Claire Wardle: Yes, I would argue that deepfakes are an example of false information disseminated to cause harm, so that would be disinformation. Misinformation might be that my mom sees that deepfake later and she reshares that. She doesn't understand that it's false. My mom's not trying to cause harm. These things can shift as they move through the ecosystem.

Mr. Frank Baylis: What is the difference between disinformation and malinformation then?

Dr. Claire Wardle: Regarding malinformation, we talk a lot about fabricated content or false content, but there is a way to use genuine content to cause harm. For example, leaking emails that were previously private and making them public might be a form of malinformation. There is a form of a whistle-blowing leak where that's done for the public good, so malinformation is to leak information to cause harm.

Mr. Frank Baylis: Like “mal” in the sense of “malicious”? Is that what you mean by “mal”?

Dr. Claire Wardle: Yes.

Mr. Frank Baylis: There's disinformation, misinformation, and malicious information, and malinformation is actually true, but it's used to distort or contort.

Dr. Claire Wardle: Yes.

Mr. Frank Baylis: To you, deepfakes would be disinformation.

Dr. Claire Wardle: Yes.

Mr. Frank Baylis: Mr. Tseng and Mr. Black, would that go along with how you see this concern about deepfakes?

Mr. Ryan Black: Largely, it does. I do agree that it's definitely a form of false information, but to attribute malice to it.... Some deepfakes are done for parody or for humour. There will almost certainly be a Hollywood version of deepfakes used to transplant actors' faces. There will be legitimate uses of deepfake, but in the news sphere or in the social media sphere, there certainly is a vulnerability that it would be used for malicious purposes. I tend to agree that it's definitely a form of falsification, just like a tricky camera angle or an edit could be disinformation as well.

Mr. Frank Baylis: What is the difference between a deepfake and just a regular fake, or a fake video and a deepfake? Could you explain that to me?

Mr. Ryan Black: Actually, I found an article through search engines that Dr. Wardle participated in, in Australia, which explains it very well. I would encourage people to hit their favourite search engine to find it.

Basically, it learns details from a series of images that are publicly sourced or sourced through other means. It learns details about the face and then uses deep-learning techniques—they're algorithmic and not logic in nature—to learn how the face interacts as it moves. Then, using a transplant victim.... If I were to take a video of Pablo here and I had enough video that had been pumped into the deepfake learning engine, I could just put my face onto Pablo's and very convincingly make Pablo look like he's talking while I'm moving.

Mr. Frank Baylis: Over time probably every kid in high school is going to be doing this, right?

Mr. Ryan Black: There are face-swap apps already.

Mr. Frank Baylis: The way we're going with this concept of deepfake, every kid's going to be doing this with their friends and making these videos, if I understand what you're saying. It's going to be that easy to do, right?

Mr. Ryan Black: It's a technology of very limitless application, and will be used for more than faces. It will be used for full bodies. At some point it will be used for transplanting entire things or other characteristics. It could be used for voice just as easily as for face as well.

Mr. Frank Baylis: Okay.

I'd like to go back to you, Ms. Wardle, for another question. I missed what you mentioned—this angry-face emoji or a crown something. What was it that you said, exactly?

Dr. Claire Wardle: If you're on Facebook and you see a piece of content, you can add a reaction. It can be a happy face or—

Mr. Frank Baylis: I know what that is.

Dr. Claire Wardle: Yes.

Mr. Frank Baylis: What were you referring to, though, when you said “crown Google” or something?

Dr. Claire Wardle: When we are searching for content we put a search filter on that says to only find us content that has a disproportionate amount of angry emoji reactions, because people have an angry emotional reaction to a lot of this deceiving content.

Mr. Frank Baylis: That leads you to a lot of the disinformation. Is that what I understand?

Dr. Claire Wardle: Yes, it leads to a lot of the false, misleading content. People who are perpetuating this understand that this is an emotional response, and so they are using material that makes you angry. If you look for those reactions, you end up finding a disproportionate number of these examples.

● (1145)

Mr. Frank Baylis: —of the disinformation or the malinformation.

Dr. Claire Wardle: Yes.

Mr. Frank Baylis: Okay. You're saying it's just a way that can be used to find them.

One last thing for you, Ms. Wardle. You had mentioned this database in the United Kingdom. What was the name of that, again?

Dr. Claire Wardle: No, it's a suggestion by Full Fact in a document they published last week, saying that we need a public database of ads. My point is they are specifically saying political ads. There are questions, of course, around how we define a political ad, when we know that the majority of the problematic content might not be directly related to a candidate; it's around other social and political issues. There's a challenge here unless we have a database of all advertising. The idea of defining political advertising will require additional thought.

Mr. Frank Baylis: If we define political advertising, we should look at what Full Fact is saying and then put in whatever way to track these things. They may be fake. They may be mal-whatever, whatever captures that, at least, within that context of who's advertising politically. There could be things outside of that, though.

Dr. Claire Wardle: Exactly. They're saying that, at a minimum, there should be a transparent database, for example on Facebook, where people are paying to promote posts—essentially a form of advertising—around an election period.

Mr. Frank Baylis: Okay.

How much time do I have left?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): You have 50 seconds.

Mr. Charlie Angus (Timmins—James Bay, NDP): Never ask; just go.

Mr. Frank Baylis: There you go. It sounds like I have a lot more.

Mr. Harris, your point about its being a whack-a-mole problem.... You've certainly done a lot of thinking about this issue. You talked about putting limits on technology. Is it possible that we have to go the other way and even go further into AI so that someone could build a device to say where you're being manipulated and how you're being manipulated? Ms. Wardle is saying to look it up on a database, and then at least make it transparent like that, but as you said, they're going to get better and better and they're going to use all this technology against us. Would the next step not be that someone could design a technology to say that if you see this ad, this is how the guy's fooling you, or if you see that ad, this is where it was posted. Have you thought along those lines of using technology to counter technology, in this sense?

Mr. Tristan Harris: Yes, this is already the case, in some sense. The human eye in the future will not be able to discern the difference when something has been algorithmically generated, where a computer generates the video or the image of the person you're speaking with. You will literally not be able to do it. You have two options. Either you try to limit the ability of people to create those kinds of deceiving things or you try to create counter-artificial intelligences to fight the AIs that are trying to deceive you.

Increasingly, we're already having to do that. The U.S. Department of Defense, I believe, was publicly.... There was an article about how they're trying to do that. In terms of a framework, I think what we need to do is start by saying that the human being is vulnerable, based on an understanding, an honest understanding and a humble understanding, of how we really work. How do we then protect ourselves from the way all technology works?

By the way, this also works for addiction and the mental health of young people and loneliness and alienation and polarization. These are all sort of on a spectrum of effects, once you understand the machinery of how we really work.

Mr. Frank Baylis: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

With our second seven minutes, we'll go to Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair, and thank you all for your testimony today. It's very helpful and adds to our accumulation of testimony.

This study has revealed the vulnerability of the electoral process pretty well anywhere in the world, and not only to the sort of psychographic microtargeting that we heard about in the Cambridge Analytica, Facebook, AggregateIQ situation, partially developed and assisted by Christopher Wylie and then revealed when he believed that they were going too far and he blew the whistle. It's also shown us about the movement of data and campaign strategies across national borders; money in and out; the creation of a multitude, or a number, of third parties to avoid spending limits and laws; and the anonymity of social media advertising in the British Brexit referendum and in any number of American political situations.

I'd like to come back, Ms. Krause, to you. You touched on it in your opening statement. I wonder if you could connect the dots for us in terms of the relationship, in the Canadian political context, between Tides Canada Leadnow and the Dogwood initiative.

● (1150)

Ms. Vivian Krause: Sure, I'd be glad to.

Let's start with Tides Canada. The American Tides Foundation, based in San Francisco, incorporated in British Columbia in the late 1990s and then changed its name to become the Tides Canada foundation. The American Tides Foundation, I think it would be fair to say, is the parent organization of Tides Canada.

The Dogwood initiative was initially created out of the American Tides Foundation. Initially it was called Forest Futures, and then it changed its name around 2004 to become Dogwood.

Leadnow, if I'm not mistaken, began around 2010 as a not-for-profit. Dogwood itself is also a not-for-profit, but it has been funded by at least 10 registered charities over the years. As I mentioned, one of the charities that funds it is the Salal Foundation. It was created by the same people, including the former chairman of the board of the Tides Foundation. For 12 years, it was dormant. It was inactive. Then, in 2012, it basically sprang to life, and Salal's revenues have now gone from about $200,000 to more than $1 million. In fact, last year, the number one top recipient of funds from Tides Canada, if I'm not mistaken, was Salal, which got $488,000.

I think what we're seeing is that in the tar sands campaign, the campaign to landlock the crude from western Canada, more than 100 organizations have been funded in the U.S., Canada and Europe. The number one and two, the top one, is the Sisu Institute Society, which funds Leadnow, and Dogwood.

Hon. Peter Kent: Does your research give any suggestion of the total amount of foreign funding, American funding it would seem primarily, that has been delivered to these various associated and aligned groups?

Ms. Vivian Krause: These are big-picture numbers. I've traced more than $600 million that has come into Canada, mostly for large-scale conservation initiatives. Of that, at least $90 million was earmarked specifically for efforts to restrict oil and gas. That's not including 2017 and 2018. Tides Canada, for example, has had more than a quarter of a billion dollars in revenue since 2009. At least $90 million of that is from outside Canada.

Hon. Peter Kent: In a number of your writings, you have suggested that it's easy for a political party to claim to take the high road in its campaign when it has third party supporters that can do the mudslinging. I'm paraphrasing the mudslinging part; I mean doing the dirty work. Is that your belief, from your research?

Ms. Vivian Krause: I've never used the words “mudslinging” or “dirty work”, but I would say that groups like Leadnow and the Dogwood initiative influence elections primarily in two ways. One is by what you might call framing the narrative, establishing the issues on which the election is fought. The second is by targeting first-time voters, people who have never voted before, young people especially, and getting them out to vote.

Hon. Peter Kent: That's through social initiative or on-the-ground paid—

Ms. Vivian Krause: It's a combination. They refer to the synergy between offline and online, and creating what they call offline events like protests at MPs' offices, marches, etc., and then photographs of those are taken and used online. Sometimes those photos are done in such a way that it looks as if there were a lot more people there than there actually were.

It's the combination between the offline events in real life and how those are then used online.

Hon. Peter Kent: You commented on the Canada Revenue Agency's interest, or lack of interest, in some of these third party organizations. At one point, the CRA was auditing a number of not-for-profits.

Ms. Vivian Krause: Registered charities—this is what the CRA audited.

Hon. Peter Kent: Registered charities.

Ms. Vivian Krause: Yes.

Hon. Peter Kent: In the CRA minister's mandate letter, there were a couple of interesting statements: “Allow charities to do their work on behalf of Canadians free from political harassment”, and “This will include clarifying the rules governing 'political activity,' with an understanding that charities make an important contribution to public debate and public policy.”

Do you believe that it was interpreted by the CRA minister to shut down the audit of some of these charitable organizations?

Ms. Vivian Krause: I don't know how the CRA interpreted that, but the fact is that the CRA has come out with a report saying it audited 42 charities for their political activity, and 41 out of the 42 were not fully compliant—41 out of 42. Since then, nothing has happened. My understanding, just from what I've heard in the media, is that the national revenue ministry has instructed the CRA to basically stand down and not follow through with any of the audit findings, and it had recommended the revocation, in other words, the complete shutdown, of five charities.

I would suggest to the committee that if you want to do something to better protect the integrity of elections, the place to start is at the CRA. The reason I say this is that in 2016 I spent eight months writing a report, which I submitted to Elections Canada. They then flew some investigators out to Vancouver and after four hours with them, basically, it was clear that Elections Canada can't do anything if the CRA allows charities to Canadianize money. Then, when those charities report their spending in their third party election reports, they report it as Canadian, because the charity has been Canadianized through charities like Tides Canada.

● (1155)

Hon. Peter Kent: Some would call that money laundering.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you for that.

I would note that I also post pictures to make it look as if there are more people at my events, when I post them on the Internet.

Mr. Charlie Angus: I've been pointing that out for months.

Voices: Oh, oh!

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Mr. Angus, you have seven minutes.

Mr. Charlie Angus: Thank you very much.

This has been a fascinating study, because we're trying to look at protection of the integrity of the electoral system, but we're starting to, I think, deal with much larger issues that are going to be much more complex for parliamentarians to consider.

Mr. Harris, I am a digital addict. My wife has called me out on that many times, especially Friday nights. I'm not allowed to go on Facebook and Twitter when I get home after a week, just to try to civilize me. I've checked my phone probably 12 times since you were talking. But I did spend half my life without digital—as a kid reading comic books, climbing trees, listening to vinyl, spending time outside the principal's office without a phone—and I'm addicted, and I accept it.

I'm concerned about the picture you're painting of the massive level at which we are jacked into these systems that are growing stronger all the time. I look at young people, and I look at kids I see in the grocery store whose mothers have given them a phone to play with. What do you think the larger long-term impacts are on brain development, on the ability to have young people develop internal spaces, about the ability to imagine and the ability to remember? Are you concerned that, as we're jacked into these much larger systems, we're actually rewiring our internal spaces?

Mr. Tristan Harris: Yes. I'm so glad you brought this up.

There are a number of issues to be concerned about, so I'm going to try and figure out how to formulate my response.

One way to look at this, if you think about protecting children.... Marc Andreessen, who is the founder of Netscape, has this insight that says software is eating the world. That means every single industry, domain, whether that's the way that children consume media or the way we get around in Ubers versus taxis, technology, if you throw it into that domain, will do the thing more efficiently. So software will continue eating the world. However, we don't regulate software, so what that really means is “deregulation is eating the world”.

I don't know how it works in Canada, but in the United States I think we still have protections about Saturday morning cartoons. We recognize there is a particular audience, which is to say, children, and we want to protect them. We don't want to let advertisers do whatever they want during the Saturday morning cartoon period.

As soon as you basically offload that regulated channel of television and formal Saturday morning programming, and say let's just let YouTube Kids handle it, then you get algorithms, just machines, where the engineers at YouTube have no idea what they're putting in front of all of those 2.2 billion channels, of which several hundred million are for children.

That's how to see the problem. We have a five-second delay on television for a reason. There are 100 million people or 50 million people on one side of the screen and a couple of people who are monitoring the five-second delay, or the editorial. If some gaffe happens, or there is profanity or something like that and you want to protect...you have some kind of filtering process.

Now we have 2.2 billion channels. This is the same, whether on the other side of that channel is a child or a vulnerable person in Myanmar who just got the Internet and is basically exposed to vulnerable things. The unified way of seeing this problem is that there is a vulnerability in the audience, whether that audience is a child, someone in Myanmar, or someone in an election. If we don't acknowledge that vulnerability, then we're going to have a huge problem.

The last thing I'll say, just to your point about children, is that when the engineers at Snapchat or Instagram—which, by the way, make the most popular applications for children—go to work every day, these are 20- to 30-year-olds, mostly male, mostly engineers, computer science or design-trained individuals, and they don't go to work every day asking how they protect the identity development of children. They don't do that. That's not what they do. The only thing they do is go to work and ask, “How can we keep them hooked? Let's introduce this thing called a “follow button”, and now these kids can go around following each other. We've wired them all up on puppet strings, and they're busy following each other all day long because we want them just to be engaged.”

● (1200)

Mr. Charlie Angus: That's where I want to go with that, because it's a question of vulnerabilities. There is the vulnerability of our electoral system to be undermined, which we're seeing can happen.

There is also the vulnerability of addictions. One of the seminal moments in the battle with cigarette companies was the revelation that they had the nicotine delivery systems built in there to continue addictions. They couldn't just say, “Well you chose to smoke. You like smoking. You're responsible for smoking.” It was the actual addictive intent of the companies.

As someone who has worked for Google, as an ethicist, what do you think we need to be looking at in terms of the addiction delivery mechanisms that are being written into code?

Mr. Tristan Harris: The first thing to say is that this is because of the attention economy and the race to gather human attention. As it gets more competitive, it's not enough that you use the product. Where I used to get your conscious choice to use it, I have to crawl deeper down the brain stem and get you addicted to it. I need to create an unconscious habit inside of you so that you basically use it every day for that 30 minutes—to own that 30 minutes.

What started with no one using these sort of slot machines, where you check your phone like a slot machine and pull down to refresh it, the second that one person does that and it works really well at keeping people hooked, other people now have to start creating all of the slot machines.

If you think of it game theoretically, each player has to go deeper and deeper down the brain stem to do this. What we need to think about is how would we regulate that addictive process and instead protect human agency and dignity, instead of basically trying to erode it deliberately.

The companies have not been honest about this, as you've said.

Mr. Charlie Angus: Thank you.

Mr. Black and Mr. Tseng, on the issue of deepfakes and the legal powers, under the Copyright Act in Canada, we have notice and notice, as opposed to notice and takedown. There has been push-back on imposing notice and takedown, because they say that you could be unfairly interfering with someone's rights, that you could be unfairly targeting a competitor.

On the question of deepfakes, are there specific legal things that we have to look at in terms of its effect on say, upending an election?

What are the legal parameters? If someone has been the subject of a deepfake, they could go the libel route. There are a number of traditional mechanisms in place that may be sufficient. But if it happens in the middle of an election, it could upend the democratic system.

Are there specific remedies that would be better able to address the threat of a deepfake, and upending elections?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Please answer very briefly.

Mr. Ryan Black: I'm not sure that deepfake technology would be an appropriate target for any specific action, only because it is one in a very large belt of tools available to people who are trying to manipulate people through social media. Through the ways that both of the other speakers have spoken about, our brains are kind of wired to heuristically solve problems that we can't possibly logically solve because there's so much information being thrown at us at all times.

I worry, truthfully, more about the intent of misinformation and disinformation. I truthfully worry more about that than the specifics of deepfake video. This is only because—again, I go back to my security camera footage—you don't need to have a very sophisticated video or fake video to convince people that something's happened. You don't need to have a very convincing photo to convince people that something's happened. You can use a real image just as easily as you can use a fake image.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

Our last seven minutes goes to Mr. Picard.

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

My first question will be for Mr. Harris.

You said, and we agree, that there is a gigantic volume of information thrown at people, to a point that it's almost impossible for us to see clearly through the information we get.

Are you saying that this enormous volume of info limits our capacity to see what's real and what's not? Does it prevent us from being able to cross-check information to a point that, as Dr. Wardle said, we damage...like losing an election? It will impact our behaviour and we will have nothing that we can do to prevent ourselves from being influenced. Therefore, we will see our behaviour impacted without our being able to do something.

● (1205)

Mr. Tristan Harris: Yes.

Obviously, people have some amount of free choice to double-confirm everything that they're reading and things like that. I try to look, as a sort of a behavioural scientist, at just the reality of human behaviour. What do most people do most of the time? The challenge is that when we are so overloaded and our attention is so finite and we're constantly anxious and checking things all the time, there really isn't that time to realistically double-check everything.

There are two kinds of persuasion. There's persuasion where if I the magician tell you how this works, suddenly the trick doesn't work anymore because you know that it's a technique. There are forms of advertising where that's happened. The second kind of persuasion is that even if I tell you what I'm doing, it still works on you. A good example of this is what Dan Ariely, the famous behavioural economist, says, that it's about flattery. If you tell someone, “I'm about to flatter you and I'm making it up,” it still feels really good when you hear it.

A second example of this is if you put on a virtual reality helmet. I know that I'm here in San Francisco in this office, but in the virtual reality helmet, it looks like I'm on the edge of a cliff. If you push me, even though my mind knows that I'm here in San Francisco, millions of years of evolution make me feel like I should not fall over.

What we have to recognize is that the socio-psychological instincts, such as those that arise when children are shown an infinite set of photos of their friends having fun without them—“I know that is a highlight reel; I know that is a distortion”—still have a psychological impact on people. The same thing is true of the kinds of toxic information or malinformation that Claire is talking about.

Mr. Michel Picard: If I still have a small capacity to tell the difference between what is false and what is right, the big difference today is.... If I go back decades ago, in the 1940s and 1950s, priests in Quebec talked to their people, saying that hell is red and the sky is blue. The priests were referring to the colour of political parties racing in the next election. At that time, the only way to have people aware of what was going on was by mail, so you had to buy stamps, or on TV or radio, so you had to buy publicity. Nowadays when you make advertisements, you use media. You can send messages to millions and millions of people with one click and no cost. It's the same game, but the volume is totally different. The tools of the 1950s are the same, but with more technology.

As a government, we have to regulate something, somehow, somewhere. What do we regulate? Do we regulate the right to say stupid stuff on the media, or do we have to regulate people because apparently they're not able to see the light through all this blackness and dark side of the web?

Mr. Tristan Harris: You have described it. We've decentralized vulnerabilities so that now, instead of waiting to pay to publish something, I just basically ride on the waves of decentralized chaos and use people's socio-psychological vulnerabilities to spread things that way.

In terms of regulation, one thing we need to think about is at what point a publisher is responsible for the information it is transmitting. If I'm The New York Times and I publish something, I'm responsible for it because I have a licence and I've trained as a journalist and could lose the credibility of being a trusted organization.

One thing the technology companies do is make recommendations. We've given them the safe provision that they're not responsible for the content that people upload, because they can't know what people are uploading. That makes sense, but increasingly, what people are watching, for example, with YouTube, 70% is driven by the recommendations on the right-hand side. Increasingly, the best way to get your attention is to calculate what should go there.

If you're making recommendations that start to veer into the billions, for example, Alex Jones' infowars conspiracy theory videos were recommended 15 billion times, at what point is YouTube, not Alex Jones, responsible for basically publishing that recommendation? I think we need to start differentiating when you are responsible for recommending things.

● (1210)

Mr. Michel Picard: With the amount of information available to me, and I can't control what's coming to me, do I have to rely only on artificial intelligence to help me see transparency through all of this?

Mr. Tristan Harris: The reality is that most people don't even know anything about what we're talking about. They think YouTube is just showing them stuff. They don't realize that when their mind lands on that YouTube video, they have just entered a chess match with a supercomputer pointed at their brain, in which their brain is the chessboard, and it knows far more moves ahead on that chessboard than they do. I think most people are not even aware of this, and that's what we have to change.

Mr. Michel Picard: As a final note, I have a comment, Mr. Chair.

I'll just mention to my honourable and very respected colleague, MP Kent, that for something to be money laundering requires knowing that the money originates from a criminal source or criminal activity. Before accusing anyone of money laundering, we have to be careful.

Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much, Mr. Picard.

We'll move to our five-minute round. The first five minutes go to Mr. Gourde.

[*Translation*]

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

My question is for all the witnesses.

From one meeting to the next since the start of this study, it has been chilling to hear everything that can be done digitally to influence people in an election. In my opinion, it is clear that we will have to legislate on this sooner or later.

Do you think it would be possible to do that effectively, in the short or medium term? To my mind, that means we would have to be ready for the election in 2019. Otherwise, would we have to ban all use of advertising and social media in the next election in order to at least be fair and equitable to all the political parties and independent candidates who are running?

Ms. Vivian Krause: Is that question for me? If I understood correctly, you want to know if all social media have to be eliminated.

Mr. Jacques Gourde: If we try to bring in effective legislation, in the short or medium term, will we have to consider banning social media in the upcoming election, to be fair and equitable to everyone running?

Ms. Vivian Krause: That does not seem feasible to me. Furthermore, since there are so many ways of using social media effectively, I do not think banning their use makes any sense. The issue is not eliminating them, but rather looking at how they are used. I think regulations are needed. I can only imagine how much people would object to that idea.

[*English*]

It would be like banning free speech.

[*Translation*]

I don't think we can do that.

Mr. Jacques Gourde: That is very interesting, but equitable legislation is needed that would provide an avenue for action. An election campaign lasts between 35 and 40 days. When those information networks are used to disseminate fake news or fake videos, that can influence Canadians tremendously. We would never have the time in an election campaign to tell people that fake news had been disseminated and that people have been affected. It will come out, but not until after the election. If we are unable to monitor the information and take action when it is fake, why do we have to accept that?

Ms. Vivian Krause: It is the funding that has to be controlled, not what people say. Freedom of speech is very important, especially during an election. What we need to eliminate is outside funding so the outcome of the election is decided by Canadians alone.

Mr. Jacques Gourde: I would like to hear from the other witnesses, please.

[*English*]

Mr. Ryan Black: If I may, in my view, the quicker route to effectively pulling the curtain back on this and giving meaningful government action towards addressing this issue is far more on the education of the public side than it is on the legislative side. I worry that any legislative tool would be a very unpopular and broad hammer that would restrict legitimate uses of social media.

However, we have seen the effectiveness of campaigns in other domains, education campaigns that educate the public, for example, about not sharing their password, not being phished online, or about protecting their information or their social insurance number. These are all things that can be done to educate people, as the witnesses have talked about, to pull back the curtain on what these technology companies are doing.

I do not believe that there will be legislation that could protect us from manipulation through social media, because if you were to ban political ads.... We used the example of the Russian video where the person was pouring bleach. In that case, it wasn't a political ad at all. It was just someone doing something that was a viral video on the Internet that provoked a reaction against feminists and the left wing, and that provoked an action against the right wing.

To me, we should educate people that we do need to take that second step to try to verify and step back from the lizard brain deep within us telling us this is true and say, “Let me apply some rational thinking to this”. I do feel that would result in some more effective means.

● (1215)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much for that.

Our next five minutes go to Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you for being here and for your testimony.

I'd like to go back to the fact that we are legislators. What we're very much interested in, in this committee, is what government can do, particularly in terms of legislation, but also in other areas.

In your testimony, I'm hearing things like a video that was made in Russia, which is outside of our jurisdiction or social construct of reality, psychological persuasion, and things like we are not rational actors.

How do we legislate? I would like all of you to respond to this. What are legislative actions that we might be able to take that could help mitigate this?

Dr. Claire Wardle: One thing I would say is, as somebody was talking about, this isn't new. In an election campaign, somebody can, the night before an election, send leaflets to a whole constituency with a false rumour about a candidate. This issue that we would legislate around content is just not possible, because a lot of this stuff is the grey, murky, misleading space.

I do think there's something specific around content that makes the election system bumble. For example, we were monitoring the election in Brazil two weeks ago. On election day, there was a great deal of rumour circulating around the fact that the machines weren't working and that you could stay at home to vote via SMS. I think if we're talking about content, that's the kind of space where there is room to say, if the harm is specifically around the election, then there is something that could be done around that.

I think we need more transparency around behaviours, not content. The platforms are moving in this direction, but they need more pressure to be placed on them in terms of what is a behaviour that we can see that we would have a problem with and we would all agree about, whether it's automation, whether the IP address is external to the Canadian border or people using fake accounts.

I think behaviour is something that is worth looking at, but the content part of this is something that is much more challenging. We need more pressure on the platforms to be more transparent about those behaviours, because we don't know what decisions they're making. It's completely opaque at the moment.

Ms. Anita Vandenbeld: Okay, go ahead.

Mr. Pablo Jorge Tseng: Speaking to Ryan's point about education, we still feel that the baseline to any good legislation is a good education that's being disseminated to the public. In addition to that, the education can obviously be supplemented by crafted legislation, which shouldn't be drafted in haste. We've seen examples in the past of what happens when legislation is drafted on a whim. It's just a nightmare for everyone. Legislation definitely should be treated as sacred and analyzed and carefully thought out before it actually comes into force.

As an example of legislation that could be expanded is what Parliament did with the Canada Elections Act, with section 480.1, which is what we were talking about earlier regarding impersonation. Just to give you a brief background, that section basically says, “Every person is guilty of an offence who, with intent to mislead, falsely represents themselves” or causes someone else to be falsely represented. Then there are a number of people who are listed: Chief Electoral Officer, election officer, people authorized to act on behalf of the office, people who are authorized to act on behalf of a registered party, and a candidate.

That's a good scope with regard to impersonation, but that's an example of perhaps a section that could be expanded to explicitly include other forms, maybe false information that's being disseminated. This is not to say this section was crafted in haste—it did target what it was intended to do—but there is room for manipulation to increase its scope.

● (1220)

Ms. Anita Vandenbeld: Mr. Harris.

Mr. Tristan Harris: One thing I would add is that the advertising business model is at the root of many of these problems.

One thing we really believe is that, if you ask people how much they've paid for their Facebook account recently, they don't even realize how it is that Facebook is worth more than $500 billion. If you imagine something like a “we are the product act”, in which companies are forced to report transparently on how much each user, each cow, is worth to them when they milk them for both their data and their attention, this would generate two things.

One is a cultural understanding of the fact that people are the product for companies based on this business model. It also selects just for the companies generating these problems, because the companies that are mostly generating these problems are ones with advertising-supported engagement business models. Culturally, it would have an impact.

The second is that, economically, people would actually start to see that they're worth $120, and that their value went up to $180 when they became a new mother. Having that transparency directly to users and directly to regulators, I think, is actually very important.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much.

For the next five minutes, we go to Mr. Kent.

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

Just to respond briefly to Mr. Picard's quibble, I think that whenever a foreign organization and foreign funds are moved into interfering situations in the Canadian electoral process, in shell companies or confected Canadian companies to misrepresent the source of that income, the term “money laundering” is quite appropriate.

Mr. Harris, I'd like to come back to you. In a profile in The Atlantic magazine, you were described as “the closest thing Silicon Valley has to a conscience”. There has been an awful lot of discussion of the social responsibility of what one of our witnesses called the “data-opolies” with regard to the imbalance between the search for revenue and profit and growing the companies versus responsible maintenance and protection of individual users' privacy.

I'm just wondering what your thoughts are on whether the big data companies do, in fact, have a conscience and a responsibility and a willingness, a meaningful willingness, to respond to some of the things we've seen coming out of, principally, the Cambridge Analytica, Facebook, AggregateIQ scandal. We know, and we've been told many times, that it's only the tip of the iceberg in terms of the potential for gross invasion of individual users' privacy.

Mr. Tristan Harris: Yes, we have to look at their business models and at their past behaviour. It wasn't until the major three technology companies were hauled to Congress in November 2017 that we even got the honest numbers about how many people, for example, had been influenced in the U.S. elections. They had claimed it was only a few million people. Claire and I both know many researchers who did lots of late work until three in the morning, analyzing datasets and saying it had to be way more people than that. Again, we didn't get the honest number that more than 126 million Americans, 90% of the U.S. voting population, were affected until after we brought them to testify.

That's actually one of the key things that caused them to be honest. I say this because they're in a very tough spot. Their fiduciary responsibility is to their shareholders, and until there's an obvious notion that they will be threatened by not being honest, we need that public pressure.

There are different issues here, but when I was at Google I tried to raise the issue of addiction. It was not taken as seriously as I would have liked, which is why I left, and it wasn't until there was more public pressure on each of these topics that they actually started to move forward.

One last thing I will say is that we can look to the model of a fiduciary. We're very worried about privacy, but we just need to break it down. I want to hand over more information to my lawyer or doctor because with more information, they can help me more. However, if I am going to do that, we have to be bound into a contract where I know for sure that you are a fiduciary to my interests. Right now, the entire business model of all the data companies is to take as much of that information as possible and then to enable some other third party to manipulate you.

Imagine a priest in a confession booth, except instead of listening carefully and compassionately and caring about keeping that information private, the only way the priest gets paid for listening to two billion people's confessions is when they allow third parties, even foreign state actors, to manipulate those people based on the information gathered in the confession booth. It's worse, because they have a supercomputer next to them calculating two billion people's confessions so when you walk in, they know the confessions you're going to make before you make them.

It's not that we don't want priests in confession booths; it's just that we don't want priests with the business model of basically having an adversarial interest manipulating your vulnerable information.

● (1225)

Hon. Peter Kent: We're told that Facebook is constructing a war room that will be intended to operate to prevent improper interference in American elections. One would think the mid-terms would be the first area that needs protection. It's not completed yet, I understand. Would you suggest that in Canada it would be advisable that Facebook establish a war room to prevent that same sort of potential interference in Canadian elections?

Mr. Tristan Harris: Absolutely. It also speaks to the global nature of the problem, which is what I was trying to get at from the beginning. For all the issues we're talking about in western developed democracies with free press reporting on these topics, there are just hundreds of vulnerable countries, as Claire mentioned regarding Brazil, that have no such apparatus. Facebook is not going to spend the money to create war rooms for every single country.

Neither do they have the engineers who speak the languages. In India, there are 22 different languages. How many of those engineers speak those 22 languages? How many of the engineers at Facebook speak Sri Lankan or Burmese, where there are actually genocides emerging from the manipulation of their platform? There's actually a dearth of civil society groups in those places. There are no civil society groups doing enough work to cover those topics.

Yes, there should be a Facebook war room in Canada. Also, structurally speaking, they're editor-in-chief of two billion people's thoughts in the morning, so how do we start to scale that out and go from unmanageable levels to manageable levels of complexity? It's a mathematical thing.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

The last five minutes go to Mrs. Fortier, who's not here. Perhaps Mr. Saini would like to take that time.

Mr. Raj Saini (Kitchener Centre, Lib.): I get the last five minutes? Okay.

Mr. Harris, I'd like to start with you, because you wrote something that I'd like some clarity on. You wrote in a couple of different places about the concept of hacking a human. Can you explain that in more detail?

Mr. Tristan Harris: Hacking probably came up with Harari, who wrote the book *Sapiens*. There's this view that in a post-enlightenment culture the customer is always right, the voter knows best or that you should trust your heart and your feelings because they are truly your own. We're increasingly living in an age where we have people on one side of the screen and supercomputer AIs on the other side of the screen who know more about us than we know about ourselves. If you think about that situation, if you enter a room and you know more about the other person's mind than they know about their own mind, who wins?

Why does magic work? It works because there's an asymmetry where the magician knows something about the limits of your mind. They can hack your mind, because they know something that you don't know about your own mind. Any time that's true, in that asymmetric situation, the party that knows more will—quote, unquote—"win".

We're enabling new forms of automated psychological influence—again, the fact that YouTube calculates what has caused two billion people to watch that next video—and we're just throwing that at new human beings every day. We say that if it works at getting you to watch the next video, then it must be good, because the customer is always right and the voter knows best. But, that's not true. We're really wiring in the lizard brain and calculating what works on lizard brains, and then showing that back to people and creating a loop.

Artificial intelligence turns correlation into causation. It used to be correlated that people who watch this now watch this, but then AI can drive that into a causative loop. The problem is that we're creating a chaos loop, because if you take feedback loops and you feed them into themselves, you get chaos as a result. That's what's happening across our social fabric by hacking humans and feeding them back into the loop.

● (1230)

Mr. Raj Saini: You gave an example in one of your articles about YouTube, and you've mentioned it here also. I'm just going to tell you about something that happened to me.

Last week, I went to a grade 5 civics class and I was speaking with them. There was a Q and A after, and some of the students in grade 5, who are 10 years old, asked me what my favourite YouTube channel or video was. When I go on YouTube, I have an interest in TED Talks, or something politically related where you're watching a speech or something, but I'm also fascinated by how quickly the right side of the screen fills up with suggested topics.

If I'm watching that stuff and I don't have an awareness, either I'm young or maybe not as knowledgeable, I'm technically being hacked. I'm being injected with information that I didn't seek. I might have tried to find something that I found of interest, through an article or an ad or something, and all of a sudden all these videos are appearing, which are furthering the original premise.

If you don't have the ability to differentiate between what is right and what is wrong, then technically that's a hack. But if you look at the amount of information that's being uploaded on any given day, how would...? You talked about regulating the information. How is it possible that YouTube can regulate that information when you have so much information being uploaded? What kind of advice could you give us as lawmakers? How would you even contemplate regulating that information?

Mr. Tristan Harris: This is why I said.... The advertising business model has incentivized them to have increasing automation and channels that are doing all this. They want to create an engagement box—it's a black box; they don't know what's inside it—where more users keep signing up, more videos keep getting uploaded, and more people keep watching videos. They want to see all those three numbers going up and up.

It's a problem of exponential complexity that they can't possibly hire trillions of staff to look at and monitor and moderate the—I forget what the number is—I think billions of hours or something like that are uploaded now every day. They can't do it.

They need to be responsible for the recommendations, because if you print something in a newspaper and you reach 10 million people, there's some threshold by which you're responsible for influencing that many people. YouTube does not have to have the right-hand side bar with recommendations. The world didn't have a problem before YouTube suddenly offered it. They just did it only because the business model of maximizing engagement asked them to do it. If you deal with the business model problem, and then you say they're responsible for those things, you're making that business model more expensive.

I think of this very much like coal or dirty-burning energy and clean-burning energy.

Right now we have dirty-burning technology companies that use this perverse business model that pollutes the social fabric. Just as with coal, we need to make that more expensive, so you're paying for the externalities that show up on society's balance sheet, whether those are polarization, disinformation, epistemic pollution, mental health issues, loneliness or alienation. That has to be on the balance sheets of companies.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

With that, we have three minutes for Mr. Angus.

Mr. Charlie Angus: Thank you.

Ms. Wardle, I want to talk about the expanse and the changing nature of disinformation. My region, my constituency, is bigger than Great Britain, so one of the easiest ways to engage with my voters is through Facebook. In my isolated indigenous communities, Facebook is how everyone talks.

There are enormous strengths to it, but I started to see patterns on Facebook. For example, there was the Fukushima radiation map showing how much radiation was in the Pacific Ocean. It was a really horrific map. I saw it on Facebook. People were asking what I was going to do about it. I saw it again and again, and I saw people getting increasingly agitated. People were asking how come no newspaper was looking at it and why the media was suppressing it, and they were saying that Obama had ordered that this map not be talked about. I googled it. It's a fake. It didn't do a lot of damage, but it showed how fast this could move.

Then there was the burka ad of the woman in the grocery store. It's in America, but then it was in England, and then it was in Canada in the 2015 election. It was deeply anti-Muslim. People I knew who didn't know any Muslim people were writing me and growing increasingly angry because they saw this horrific woman in a burka abusing a mother of a soldier. That also was a fake, but where did it come from?

Now we have Myanmar, where we're learning how the military set up the accounts to push a genocide. When we had Facebook here, they kind of shrugged and said, “Well, we admit we're not perfect.”

We're seeing an exponential weaponization of disinformation. The question is, as legislators, at what point do we need to step in? Also, at what point does Facebook need to be held more accountable so that this kind of disinformation doesn't go from just getting people angry in the morning when they get up to actually leading to violence, as we've seen in Myanmar?

● (1235)

Dr. Claire Wardle: A big part of our focus ends up being on technology, but we also need to understand what this technology sits on top of, and if we don't understand how societies are terrified by these huge changes we're seeing, which we can map back to the financial crisis.... We're seeing huge global migration shifts, so people are worried about what that does to their communities. We're seeing the collapse of the welfare state. We're also seeing the rise of automation, so people are worried about their jobs.

You have all of that happening underneath, with technology on top of that, so what is successful in terms of disinformation campaigns is content that reaffirms people's world views or taps into those fears. The examples that you gave there are around fears.

Certainly, when we do work in places such as Nigeria, India, Sri Lanka and Myanmar, you have communities that are much newer to information literacy. If we look at WhatsApp messages in Nigeria, we see that they look like the sorts of spam emails that were circulating here in 2002, but to Tristan's point, in the last 20 years many people in western democracies have learned how to use heuristics and cues to make sense of this.

To your point, this isn't going anywhere because it feeds into these human issues. What we do need is to put pressure onto these companies to say that they should have moderators in these countries who actually speak the languages. They also need to understand what harm looks like. Facebook now says that if there's a post in Sri Lanka that is going to lead to immediate harm, to somebody walking out of their house and committing an act of violence, they will take that down. Now, what we don't have as a society is to be able to say, what does harm look like over a 10-year period, or what do memes full of dog whistles actually have in terms of a long-term impact?

I'm currently monitoring the mid-term elections in the U.S. All of the stuff we see every single day that we're putting into a database is stuff that it would be really difficult for Facebook to legislate around right now, because they would say, “Well, it's just misleading” and “It's what we do as humans”. What we don't know is what this will look like in 10 years' time when all of a sudden the polarization that we currently have is even worse and has been created by this drip-feed of content.

I'll go back to my point at the beginning and say that we have so little research on this. We need to be thinking about harm in those ways, but when we're going to start thinking about content, we need to have access to these platforms so we can make sense of it.

Also, as society, we need groups that involve preachers, ethicists, lawyers, activists, researchers and policy-makers, because actually what we're facing is the most difficult question that we've ever faced, and instead we're asking, as Tristan says, young men in Silicon Valley to solve it or—no offence—politicians in separate countries to solve it. The challenge is that it's too complex for any one group to solve.

What we're looking at is that this is essentially a brains trust. It's cracking a code. Whatever it is, we're not going to solve this quickly. We shouldn't be regulating quickly, but there's damage.... My worry is that in 20 years' time we'll look back at these kinds of evidence proceedings and say that we were sleepwalking into a car crash. I think we haven't got any sense of the long-term harm.

Mr. Charlie Angus: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

We have just over 20 minutes left. I would propose that we do five minutes and see where we get.

Hon. Peter Kent: Sure.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): If you don't mind, I'll start, because I'm stuck in this chair and I don't get to ask as many questions as I'm used to.

I'll start with Ms. Wardle.

I take no great offence to your thinking that politicians can't quite figure it out, but we are where we are. We have to make recommendations to the government as to what they need to do. I should note that they have bolstered an act to require online platforms to create a registry of all digital ads placed by political or third parties during pre-writ and writ periods. That's to your point about a registry. We have already made a recommendation with respect to transparency of advertising, which I think is a critical piece in conjunction with that registry, so that there's a real-time honesty in ads.

What other specific recommendation would you have? Put yourself in our shoes and say, “Government, specifically beyond the registry, beyond honest advertising, this is another piece that you should be recognizing about the limitations of empirical evidence.”

● (1240)

Dr. Claire Wardle: I would also say that we need to support quality journalism. They are part of this ecosystem. There are significant issues around local news deserts. If we don't recognize the connection between local journalism collapsing and the fact that local communities are turning to Facebook as their only source of information, we have a problem.

I'll give a plug now. In Brazil, we've created a coalition of 24 major newsrooms that are working together in a way that newsrooms never do. They normally compete, but there's no reason to compete around disinformation. I have 24 newsrooms that work collaboratively every day to find, verify and write debunks on one central website. Their logos are next to each other to show the audience that it doesn't matter about their political perspective, this is a false piece of content. It's amplified through their own 24 channels, online sites, radio, television and social media channels.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

Dr. Claire Wardle: I was going to say....

The Vice-Chair (Mr. Nathaniel Erskine-Smith): I'm sorry, but I only have five minutes. I want to come back to you.

Mr. Harris, you talked about redesigning and realigning tech, given human limitations. You've talked a lot about the problem. Let's take the same question to you, about a specific policy prescription that you would want this committee to recommend to the government.

Mr. Tristan Harris: Yes, I think we should always be skeptical anywhere that governments would tell companies how to design their products. That's not the place of the government. What I was mostly talking about in that earlier statement was that there are ways to design products that protect a vulnerability in the human animal.

If we know that a slot-machine style of social validation which doses kids every 15 minutes has this addictive effect and generates fear of missing out, we could start by understanding that kids are vulnerable to that, and design to protect against that addiction.

If we know that colour rewards light up your brain, and notifications buzzing against human skin at a certain frequency and rate tend to stimulate anxiety in your nervous system, we can start by understanding that there's a different way to design and protect against that happening.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): How do we put that into a rule? How do we take those ideas and....

Mr. Tristan Harris: Those are examples of how the design should work, but that's different from what we would legislate. I'm not saying we should legislate that. We shouldn't tell Apple how to design their products legislatively, but I think we need to make them responsible for the externalities that they generate in society.

We have a project called the ledger of harms. I don't want to promote it or anything like that, but we think we need to show the ledger of harms across the social fabric that are being externalized onto society, and that never show up on the balance sheets of companies. It's not because these are evil companies. They just can't see the harm they're generating, like any polluting company.

These harms are subtler. They're epistemic harms in how we know what we know. They're polarization harms. They're alienation, isolation, belonging, community, children, mental health, teen suicide. These are all things that are being externalized onto the fabric of society and we need more research, more funding of that research, to show what those harms are. We need more transparency, because often the only way to know about those harms is to get access to the raw data.

They'll skeptically call Claire and me and all of us “alarmists” because we're operating on the wrong data. We don't have access to the internals. Those are the kinds of things we can do.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Going back to you, Ms. Wardle, you talked about content as a very difficult thing to police. I think that's right, but we do police content with respect to harassment. We do police content with respect to hate, but those mechanisms are insufficient to tackle the scale of the problem on the Internet.

When we ask Facebook and Google and these companies to police themselves, I wonder if that's the most effective solution. Do you have a better policy prescription for how we police the existing rules on the Internet?

Dr. Claire Wardle: You're right to make a distinction between illegal speech and legal speech.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): That's right.

Dr. Claire Wardle: I would argue that when we talk about this, everything gets lumped into legal speech.

Whether it's specifically false information or disinformation or a false piece of content around a particular politician—although that's very hard because a lot of this is just misleading, and it's partly how campaigns are fought—I think there is a sliver of false content connected to election integrity that should be put into illegal speech.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

Before I pass it to Mr. Kent, I just want to note, Ms. Krause, you'll be very pleased to know that in Bill C-76 the government will be banning advocacy groups from ever using money from foreign entities to conduct partisan campaigns. That should answer that concern you raised with us today.

Mr. Kent, you now have five minutes.

Hon. Peter Kent: Thank you, Chair.

Following on the recommendations of the advertising registry, the source of funds and so forth, I'd like to come back to you, Ms. Krause, and the point you made regarding an Elections Canada investigation which was effectively stumped by the lack of CRA detail.

We seem to be dealing with silos in terms of how to better protect the Canadian electoral process from the vulnerability that we've seen, whether it's with a Cambridge Analytica, Facebook, AggregateIQ style of scandal, or the source of foreign funding or any of these other complications.

We have a Privacy Commissioner with limited authority in one silo. We have the Chief Electoral Officer in another silo, unable to effectively investigate. We have a Commissioner of Lobbying. Until we posed a question to the chief Canadian officer of Facebook, they did not have a registered lobbyist in Canada but had made many contacts with senior ministers and chief and senior decision-making officials in the government.

What would your recommendations be to at least reduce the vulnerability of the Canadian electoral process?

● (1245)

Ms. Vivian Krause: I can only speak to the particular area that I am familiar with, which is the use of funds via charities.

When you look at the reporting in the 2015 federal election, the top advertisers, the ones that were all funded as part of the tar sands campaign, if you grouped them together, they were the number one biggest advertiser. If you take those top six groups, they reported more than half a million dollars. That was more than even the United Steelworkers. That's why I looked at that. They weren't way down the list; they were at the top of the list.

In terms of recommendations, yes, ironically it seems to me that the problem and the solution start at the CRA, not Elections Canada.

A couple of other things would help, too. One of them is in the Elections Act, where there is a section that lists things a third party advertiser needs to report their spending on, and a list of things that they don't need to report.

Right now, for instance, the creation of websites is on the list of expenditures they don't need to report. My understanding is that this is because that part of the act was written more than 10 years ago, when expenditures on that were small and not very relevant. I think we need to update and remove that. It is now not a small part of the election spending budget, but in fact the main part.

That would be one thing that could be done.

Hon. Peter Kent: To your knowledge, when the CRA began the audit of the charitable organizations, were they looking at not only foreign funds that were coming into organizations like Tides Canada, the Dogwood initiative and Leadnow, but how that money was then converted and transformed and eventually spent in the variety of ways that it could be spent in an election campaign?

Ms. Vivian Krause: I have no knowledge of how the CRA conducted any of its audits. The only thing I can tell you is that the charity at the centre of the fuss was Tides Canada. In their financial statements for 2016-17 they state that yes, the foundation was audited, but only for 2008-09. If true, it means, as I understand it, that in fact they weren't audited for any of the relevant years.

I think that the place—

Hon. Peter Kent: You say “relevant years”. Would those be election years?

Ms. Vivian Krause: Well, it would be for any of the years wherein evidence was brought to the attention of the CRA about violations of the Income Tax Act.

Just to sum up, the CRA did 42 audits. The recommendations were to shut down at least five—some say seven—of those charities. Why hasn't that happened? The CRA got more than $10 million specifically earmarked for doing that. Why were those audits not followed through on?

As one concrete, easily actionable thing that the government can do, just ask why this hasn't been completed.

Hon. Peter Kent: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much. You were just a few seconds under. Excellent job.

Next is Mr. Angus for five minutes.

Mr. Charlie Angus: It's okay. He's gifted his few seconds to his left-wing colleague.

● (1250)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Just use them.

Voices: Oh, oh!

Mr. Charlie Angus: Yes. Thanks.

Mr. Harris, I was interested in your comments that we have to move beyond this whack-a-mole approach, so I'll ask a question about the size of these platforms.

You said you were in a start-up that was purchased by Google. Is that correct?

Mr. Tristan Harris: Yes.

Mr. Charlie Angus: Okay. Then you mentioned you had friends who worked for Instagram, which is now owned by Facebook.

Mr. Tristan Harris: Yes. They just resigned from Facebook.

Mr. Charlie Angus: Yes.

The antitrust issue is at the edge of our study, but to me we keep coming back to it because of the massive power of these data-opolies that is beyond anything, in terms of a corporate size and power, that's ever been dealt with before. The power of these companies to manipulate or to be manipulated by third party actors to me is a serious question. They talk about the “kill zone" of innovation that has now arisen around the big data-opolies—

Mr. Tristan Harris: Yes.

Mr. Charlie Angus: —because of just even their AI power to anticipate potential, competitive threats and to put them out of business.

Based on your own experience, having been bought out by Google, what do we need to look at in terms of the competitive market to ensure that these companies are not able to shut down competition? Do we need to go to some form of antitrust regulation?

Mr. Tristan Harris: Actually, this is an excellent area that we probably won't be able to get too deeply into in the limited time we have. I recommend my colleague Roger McNamee, who's been doing a lot of active work on that in the Open Markets Institute in the United States.

You're absolutely right. We were a tiny start-up company, so we're not really so relevant to that conversation. But the point is that if you were trying to build an alternative to Facebook, YouTube or Twitter, it would be very hard for you to succeed because these are built on network effects. In Senator Mark Warner's policy paper that came out on his policy prescriptions, he talked about the need for interoperability. You need to be able to move interoperably between these networks. This actually happened in the late 1990s with AOL Instant Messenger. It used to be that AOL had the most popular messaging application, AOL Instant Messenger, and it was locked in. The reason everybody had to use AOL is that they had to use AOL Instant Messenger. Then they were forced, with legislation, to make that interoperable, and that helped loosen the monopoly that AOL had at the time on essentially these Internet services.

I think we need to look at similar things like that. What's harder with social networks is that you can't just move my data off to something else because my data is connected to all the posts I've made in other people's profiles and they have privacy settings so that I can't simply migrate over onto some new platform. I think this is a really important area, and it does have to do with the consolidation of power and the ability for them to quash competition.

One last thing is that Facebook has a thing called Onavo, which is a VPN tracking service. They can actually track rising competitors that are using their platforms. By knowing which ones are up and coming, they can basically start to steal their features or shut them down. There are different competitive tactics they can use.

Mr. Charlie Angus: Thank you.

Ms. Wardle, I am really interested in your comments about the potential sleepwalking into a long-term social car crash here. We've always had moral panics whenever there's a change in technology, whenever there's uncertainty, and I certainly am wary about politicians jumping in to try to prevent change. You raised the issue about the need for research, the need to be able to track this. I'm concerned when we see the rise of deeply misogynist acts online; the rise of extremism; hell, the rise of Donald Trump, the Twitter president.

What would you recommend in terms of long-term research? Where do we need to be looking at to start drawing a clear picture of the impacts of this digital realm that we're now living in, which has gone from utopian to very dystopian very quickly?

Dr. Claire Wardle: I could not agree more. The fact that we are having all these conversations, and you're potentially going to regulate something that we know almost nothing about—we've never had anything like that before. We know that there is an issue here, but that it's impossible for us to do anything about it. Even just trying to find content around the U.S. mid-terms, it's very difficult to even see some of the messages that are circulating.

I would argue, actually, around the election setting up a specific research unit that can work with the platforms to essentially put pressure on them and to say, “For this particular election, we need to work with you in a way that we understand who's saying what, and what they do as a result of that.” We can't keep saying, “We need data, we need data”, and then the platforms say, “But we can't possibly give you data because of privacy concerns.” We're stuck in this continuous loop.

To be honest, governments are the only ones right now that can put pressure on them to say that, in order for us to understand this... and even to say, “We will not regulate you until we understand it, so please give us the data so we can understand it”. I do think we need something. Around an election, they understand that elections integrity is where they're most vulnerable. I would argue that actually getting that data would make a difference.

● (1255)

Mr. Charlie Angus: Thank you very much.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much, although I would note that when we've said please to Facebook before, they haven't exactly responded.

The last five minutes go to Mr. Baylis.

Mr. Frank Baylis: Mr. Harris, I'm going to follow on what Charlie Angus was talking about with regard to these data-opolies, these large companies with all this data. Have you thought about how they have used.... Basically, they've become massive, but they've done it on the backs of copyright material that they've made use of through safe harbour rules. Newspapers are dying. Artists, musicians, photographers and writers— basically, they take all their stuff for free and put it on Facebook. If they know you like this kind of picture, they put you together with that through this algorithm.

There's been a shift of money, but the shift of money has happened massively to these five or six large companies because they have not paid any of these people who create the content that our eyeballs are after. They say, “We know you're after eyeballs”, so you're after this, you're after that, or he's after this, she's after that. They can get it for free. They don't pay for it, whereas before they had to pay for it. They just take it. They show it to you. They throw an ad in, and they make some more money.

Have you thought about if we were to enforce copyright laws completely differently, or take away safe harbour or really hammer into them that they can't take all of this for free, would that have a huge impact, or not, on these large organizations?

Mr. Tristan Harris: You know, I'm not an expert on the Copyright Act and related sorts of discussions. I will say there's a great set of work done by Glen Weyl and Jaron Lanier that just came out in a Harvard Business Review article, where they recommend a way in which people can be compensated for all the work that they're doing. This is one part of the solution.

You could think of this like it's the Industrial Revolution. Essentially you have automation, where all the profits go those who automate, the people who run the big factories, and the wage labour stays the same and they try to hold those wages down so they don't make any more money. Right now we're the labourers. Every single thing we do, everything we click on, all the data that we give, and everything we've clicked on and shared basically gets fed to these companies. They profit from it, and it hollows out the places where that money used to go. One solution is to basically make sure that people are compensated for their participation, which treats them more as a human agent with dignity, as a worker, as opposed to a cow which is being manipulated for milk. There's a great article by Glen Weyl and Jaron Lanier that's just on that.

Mr. Frank Baylis: Do they touch on the concept of ownership of your data as well: It's my data, I own it?

Mr. Tristan Harris: They do, yes. They talk about it much like a blood donor versus giving your liver. You can give out your data, but you basically maintain your protection of yourself and your data.

Mr. Frank Baylis: Thank you.

Ms. Krause, as my colleague pointed out, the latest Bill C-76 is looking to stop foreign money coming in. They were originally allowed to spend a small amount of money. We've since reduced it to zero.

You've touched on something which is an open door, if I understand it. A charity in a foreign country can give a charity in Canada the money. Then the charity in Canada can spend the money, without any constraints. Did I understand that correctly?

Ms. Vivian Krause: Yes. That's the problem. That's the loophole. That's why, when I spoke with the investigators at Elections Canada, they said, “Look, our hands are tied. In our eyes, that money is Canadian because it came through a Canadian charity.”

Mr. Frank Baylis: Is the loophole that they're able to use...? If I'm a foreign charity and I want to impact something in Canada, I'd just find a Canadian, set up a little charity in Canada, then I'd just flow the money there, $1 million, $2 million. I'd give it to them and say, “Now, you spend it in Canada.” Essentially, the money and even the directions could be coming from a foreign country.

Ms. Vivian Krause: Yes.

Mr. Frank Baylis: What law would you suggest we look at? Are there any examples elsewhere of what people have done to stop that from happening?

Ms. Vivian Krause: Sure. I think it's very simple. The Income Tax Act specifies very clearly that charities are to operate for purposes that are exclusively charitable—not mostly charitable or a little bit charitable or good, but charitable—as defined by law. So all that is required, as I understand it, is that the charities directorate of the CRA enforce the existing law.

Mr. Frank Baylis: Let's say I'm a charity for the environment. I really believe in the environment, and I really want to help polar bears or whatever. That's a political argument too, because different political parties would deal with that issue differently. In that sense I can't stop them from advocating. They are obviously going to be advocating for what they believe in, say, a tax on pollution or no tax on carbon or whatever. How would I say to them that they are not a charity, then?

● (1300)

Ms. Vivian Krause: No problem: The problem isn't political activity; the problem is political activity that does not serve a charitable purpose.

Charities have always been allowed to do political activity, but this whole discussion has been off-kilter, because it hasn't been said that, yes, charities can do political activity but political activity that furthers a charitable purpose. If it doesn't further a charitable purpose, then the allowable political activity isn't 10% or 20%; it's zero. The emphasis has been not on the political activity but on the charitable purpose.

I would actually like to see all limits on political activity removed as long as it's serving a charitable purpose. If it's serving a charitable purpose, then I think the charities should be free to pursue whatever means are most cost-effective to serving charitable purposes.

The CRA has taken more than 10 years—

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We unfortunately are out of time, but I really appreciate your comments.

I appreciate the comments of all of our witnesses today. I'm sure individual MPs will follow up with you where necessary, where people have follow-up questions. If you have any additional information you want to provide to the committee, please provide it in writing to the clerk.

With that, thank you very much.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

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

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

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

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

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

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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