HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 154 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 28, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 28, 2019

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): We'll call to order the Standing Committee on Access to Information, Privacy and Ethics for meeting 154, an by extension, the international grand committee on big data, privacy and democracy.

I don't need to go through the list of countries that we have already mentioned, but I will go through our witnesses very briefly.

From the Office of the Privacy Commissioner of Canada, we have Mr. Daniel Therrien, the Privacy Commissioner of Canada.

As an individual, we have Joseph A. Cannataci, special rapporteur on the right to privacy for the United Nations.

We are having some challenges with the live video feed from Malta. We'll keep working through that. I'm told by the clerk that we may have to go to an audio feed to get the conversation. We will do what we have to do.

Also we'd like to welcome the chair of the United States Federal Election Commission, Ellen Weintraub.

First of all, I would like to speak to the meeting's order and structure. It will be very similar to that of our first meeting this morning. We'll have one question per delegation. The Canadian group will have one from each party, and we'll go through until we run out of time with different representatives to speak to the issue.

I hope that makes sense. It will make sense more as we go along.

I would like to thank the members who came to our question period today. I personally thank the Speaker for recognizing the delegation.

I'll give Mr. Collins the opportunity for to open it up.

Mr. Collins.

Mr. Damian Collins (Chair, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you.

Let me put my first question to all three of the witnesses.

The Chair: Shall we have statements first?

Mr. Damian Collins: Okay.

The Chair: We'll have opening statements. We'll start with Mr. Therrien.

Go ahead for 10 minutes.

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair.

Members of the grand committee, thank you for the invitation to address you today.

My remarks will address three points that I think go to the heart of your study: first, that freedom and democracy cannot exist without privacy and the protection of our personal information; second, that in meeting the risks posed by digital harms, such as disinformation campaigns, we need to strengthen our laws in order to better protect rights; lastly, I will share suggestions on what needs to be done in Canada, as I'm an expert in Canadian privacy regulation, so that we have 21st century laws in place to ensure that the privacy rights of Canadians are protected effectively.

I trust that these suggestions made in a Canadian context can also be relevant in an international context.

As you know, my U.K. counterpart, the Information Commissioner's Office, in its report on privacy and the political process, clearly found that lax privacy compliance and micro-targeting by political parties had exposed gaps in the regulatory landscape. These gaps in turn have been exploited to target voters via social media and to spread disinformation.

[*Translation*]

The Cambridge Analytica scandal highlighted the unexpected uses to which personal information can be put and, as my office concluded in our Facebook investigation, uncovered a privacy framework that was actually an empty shell. It reminded citizens that privacy is a fundamental right and a necessary precondition for the exercise of other fundamental rights, including democracy. In fact, privacy is nothing less than a prerequisite for freedom: the freedom to live and develop independently as individuals, away from the watchful eye of surveillance by the state or commercial enterprises, while participating voluntarily and actively in the regular, day-to-day activities of a modern society.

[*English*]

As members of this committee are gravely aware, the incidents and breaches that have now become all too common go well beyond matters of privacy as serious as I believe those to be. Beyond questions of privacy and data protection, democratic institutions' and citizens' very faith in our electoral process is now under a cloud of distrust and suspicion. The same digital tools like social networks, which public agencies like electoral regulators thought could be leveraged to effectively engage a new generation of citizens, are also being used to subvert, not strengthen, our democracies.

The interplay between data protection, micro-targeting and disinformation represents a real threat to our laws and institutions. Some parts of the world have started to mount a response to these risks with various forms of proposed regulation. I will note a few.

First, the recent U.K. white paper on digital harms proposes the creation of a digital regulatory body and offers a range of potential interventions with commercial organizations to regulate a whole spectrum of problems. The proposed model for the U.K. is to add a regulator agency for digital platforms that will help them develop specific codes of conduct to deal with child exploitation, hate propaganda, foreign election interference and other pernicious online harms.

Second, earlier this month, the Christchurch call to eliminate terrorist and violent extremist content online highlighted the need for effective enforcement, the application of ethical standards and appropriate co-operation.

Finally, just last week here in Canada, the government released a new proposal for an update to our federal commercial data protection law as well as an overarching digital charter meant to help protect privacy, counter misuse of data and help ensure companies are communicating clearly with users.

● (1535)

[*Translation*]

Underlying all these approaches is the need to adapt our laws to the new realities of our digitally interconnected world. There is a growing realization that the age of self-regulation has come to an end. The solution is not to get people to turn off their computers or to stop using social media, search engines, or other digital services. Many of these services meet real needs. Rather, the ultimate goal is to allow individuals to benefit from digital services—to socialize, learn and generally develop as persons—while remaining safe and confident that their privacy rights will be respected.

[*English*]

There are certain fundamental principles that I believe can guide government efforts to re-establish citizens' trust. Putting citizens and their rights at the centre of these discussions is vitally important, in my view, and legislators' work should focus on rights-based solutions.

In Canada, the starting point, in my view, should be to give the law a rights-based foundation worthy of privacy's quasi-constitutional status in this country. This rights-based foundation is applicable in many countries where their law frames certain privacy rights explicitly as such, as rights, with practices and processes that support and enforce this important right.

I think Canada should continue to have a law that is technologically neutral and principles based. Having a law that is based on internationally recognized principles, such as those of the OECD, is important for the interoperability of the legislation. Adopting an international treaty for privacy and data protection would be an excellent idea, but in the meantime, countries should aim to develop interoperable laws.

We also need a rights-based statute, meaning a law that confers enforceable rights to individuals while also allowing for responsible innovation. Such a law would define privacy in its broadest and truest sense, such as freedom from unjustified surveillance, recognizing its value in correlation to other fundamental rights.

Privacy is not limited to consent, access and transparency. These are important mechanisms, but they do not define the right itself. Codifying the right, in its broadest sense, along the principles-based and technologically neutral nature of the current Canadian law would ensure it can endure over time, despite the certainty of technological developments.

One final point I wish to make has to do with independent oversight. Privacy cannot be protected without independent regulators and the power to impose fines and to verify compliance proactively to ensure organizations are truly accountable for the protection of information.

This last notion, demonstrable accountability, is a needed response to today's world, where business models are opaque and information flows are increasingly complex. Individuals are unlikely to file a complaint when they are unaware of a practice that may harm them. This is why it is so important for the regulator to have the authority to proactively inspect the practices of organizations. Where consent is not practical or effective, which is a point made by many organizations in this day and age, and organizations are expected to fill the protective void through accountability, these organizations must be required to demonstrate true accountability upon request.

What I have presented today as solutions are not new concepts, but as this committee takes a global approach to the problem of disinformation, it's also an opportunity for domestic actors—regulators, government officials and elected representatives—to recognize what best practices and solutions are emerging and to take action to protect our citizens, our rights, and our institutions.

Thank you. I look forward to your questions.

● (1540)

The Chair: Thank you once again, Mr. Therrien.

We're going to double-check whether Mr. Cannataci is able to stream. No.

We'll go next to Ms. Weintraub for 10 minutes.

Ms. Ellen Weintraub (Chair, United States Federal Election Commission): Thank you.

The Chair: I'm sorry, Ms. Weintraub.

We just heard the comments. He's available to speak.

My apologies, Ms. Weintraub. I guess we have him on, so we'll go ahead.

Mr. Cannataci, go ahead for 10 minutes.

Professor Joseph A. Cannataci (Special Rapporteur on the Right to Privacy, United Nations, As an Individual): Thank you very much, Mr. Chair, and members of the grand committee, for the invitation to speak.

I will try to build on what Mr. Therrien has said in order to cover a few more points. I will also make some references to what other witnesses presented previously.

First, I will be trying to take a more international view, though the themes that are covered by the committee are very global in nature. That's why when it comes to global...the previous witness spoke about an international treaty. One of the reasons, as I will be explaining, that I have decided in my mandate at the United Nations to go through a number of priorities when it comes to privacy is that the general framework of privacy and data protection in law insofar as an international treaty is concerned, who regulates this, doesn't happen to be specifically a UN treaty. It happens to be convention 108 or convention 108+, which is already ratified by 55 nations across the world. Morocco was the latest one to present its document of ratification yesterday.

When people meet in Strasbourg or elsewhere to discuss the actions and interoperability within an international framework, there are already 70 countries, ratified states and observer states, that will discuss the framework afforded by that international legal instrument. I would indeed encourage Canada to consider adhering to this instrument. While I am not an expert on Canadian law, I have been following it since 1982. I think Canadian law is pretty close in most cases. I think it would be a welcome addition to that growing group of nations.

As for the second point that I wish to make, I'll be very brief on this, but I also share preoccupations about the facts on democracy and the fact that the Internet is being increasingly used in order to manipulate people's opinions through monitoring their profiles in a number of ways. The Cambridge Analytica case, of course, is the classic case we have for our consideration, but there are other cases too in a number of other countries around the world.

I should also explain that the six or seven priorities that I have set for my United Nations mandate to a certain extent summarize maybe not all, but many of the major problems that we are facing in the privacy and data protection field. The first priority should not surprise you, ladies and gentlemen, because it relates to the very reasons that my mandate was born, which is security and surveillance.

You would recall that my United Nations mandate was born in the aftermath of the Snowden revelations. It won't surprise you, therefore, that we have dedicated a great deal of attention internationally to security and surveillance. I am very pleased that Canada participates very actively in one of the fora, which is the International Intelligence Oversight Forum because, as the previous witness has just stated, oversight is a key element that should be addressed. I was also pleased to see some significant progress in the Canadian sphere over the past 12 to 24 months.

● (1545)

There is a lot to be said about surveillance, but I don't have much left of my 10 minutes so I can perhaps respond to questions. What I will restrict myself to saying at this stage is that globally we see the same problems. In other words, we don't have a proper solution for jurisdiction. Issues of jurisdiction and definitions of offences remain some of the greatest problems we have, notwithstanding the existence of the Convention on Cybercrime. Security, surveillance and basically the growth of state-sponsored behaviour in cyberspace are still a glaring problem.

Some nations are not very comfortable talking about their espionage activities in cyberspace, and some treat it as their own backyard, but in reality, there is evidence that the privacy of hundreds of millions of people, not in just one country but around the world, has been subjected to intrusion by the state-sponsored services of one actor or another, including most of the permanent powers of the United Nations.

The problem remains one of jurisdiction and defining limits. We have prepared a draft legal instrument on security and surveillance in cyberspace, but the political mood across the world doesn't seem conducive to major discussions on those points. The result is that we have seen some unilateral action, for example, by the United States with its Cloud Act, which has not seen much take-up at this moment in time. However, regardless of whether unilateral action would work, I encourage discussion even on the principles of the Cloud Act. Even if it doesn't lead to immediate agreements, the very discussion will at least get people to focus on the problems that exist at that stage.

I will quickly pass to big data and open data. In the interests of the economy of time, I refer the committee to the report on big data and open data that I presented to the United Nations General Assembly in October 2018. Quite frankly, I would advise the committee to be very wary of joining the two in such a way that open data continues to be a bit like a mother with an apple pie when it comes to politicians proclaiming all the good it's going to do for the world. The truth is that in the principles of big data and open data, we are looking at key fundamental issues when it comes to privacy and data protection.

In Canadian law, as in the law of other countries, including the laws of all those countries that adhere to convention 108, the purpose specification principle that data should be collected and used only for a specified or compatible purpose lives on as a fundamental principle. It also lives on as a principle in the recent GDPR in Europe. However, we have to remember that in many cases, when one is using big data analytics, one is seeking to repurpose that data for a different purpose. Once again, I refer the committee to my report and the detailed recommendations there.

At this moment in time, I have out for consultation a document on health data. We are expecting to debate this document, together with recommendations, at a special meeting in France on June 11 and 12. I trust there will be a healthy Canadian presence at that meeting too. We've received many positive comments about the report. We're trying to build an existing consensus on health data, but I'd like to direct the committee's attention to how important health data is. Growing amounts of health data are being collected each and every day with the use of smart phones and Fitbits and other wearables, which are being used in a way that really wasn't thought about 15 or 20 years ago.

Another consultation paper I have out, which I would direct the committee's attention to, is on gender and privacy. I'm hoping to organize a public consultation. It has already started as an online consultation, but I am hoping to have a public meeting, probably in New York, on October 30 and 31. Gender and privacy continues to be a very important yet controversial topic, and it is one in which I would welcome continued Canadian contribution and participation.

● (1550)

I think you would not be surprised if I were to say that among the five task forces I established, there is a task force on the use of personal data by corporations. I make it a point to meet with the major corporations, including Google, Facebook, Apple, Yahoo, but also some of the non-U.S. ones, including Deutsche Telekom, Huawei, etc., at least twice a year all together around a table in an effort to get their collaboration to find new safeguards and remedies for privacy, especially in cyberspace.

This brings me to the final point I'll mention for now. It's linked to the previous one on corporations and the use of personal data by corporations. It's the priority for privacy action.

I have been increasingly concerned about privacy issues, especially those affecting children as online citizens from a very early age. As the previous witness has borne witness, we are looking at some leading new and innovative legislation, such as that in the United Kingdom, not only the one on digital harms, but also one about age-appropriate behaviour and the liability of corporations. I am broaching these subjects formally next with the corporations at our September 2019 meeting. I look forward to being able to achieve some progress on the subject of privacy and children and on greater accountability and action from the corporations in a set of recommendations that we shall be devising during the next 12 to 18 months.

I'll stop here for now, Mr. Chair. I look forward to questions.

The Chair: Thank you, Mr. Cannataci.

We'll go now to Ms. Weintraub.

I just want to explain what the flashing lights are. In the Canadian Parliament the flashing lights signal that votes are to happen in about 30 minutes. We have an agreement among our parties that one member from each party will stay, and the rest are clear to go and vote. The meeting will continue with the rest of us. We won't stop. It isn't a fire alarm. We're good to go.

● (1555)

Mr. Charlie Angus (Timmins—James Bay, NDP): Being the only New Democrat, as The Clash would say, should I stay or should I go?

Voices: Oh, oh!

The Chair: You probably should stay.

It's been cleared that we have one member for—

Mr. Charlie Angus: If I leave, you're not taking one of my seats.

The Chair: I just wanted to make it clear that's what's going on.

We'll go to Ms. Weintraub now for 10 minutes.

Ms. Ellen Weintraub: Thank you, Mr. Chair and members of the committee.

I am the chair of the Federal Election Commission in the United States. I represent a bipartisan body, but the views that I'm going to express are entirely my own.

I'm going to shift the topic from privacy concerns to influence campaigns.

In March of this year, special counsel Robert S. Mueller III completed his report on the investigation into Russian interference in the 2016 presidential election. Its conclusions were chilling. The Russian government interfered in the 2016 presidential election in sweeping and systemic fashion. First, a Russian entity carried out a social media campaign that favoured one presidential candidate and disparaged the other. Second, a Russian intelligence service conducted computer intrusion operations against campaign entities, employees and volunteers, and then released stolen documents.

On April 26, 2019, at the Council on Foreign Relations, FBI director Christopher A. Wray warned of the aggressive, unabated, malign foreign influence campaign consisting of “the use of social media, fake news, propaganda, false personas, etc., to spin us up, pit us against each other, sow divisiveness and discord, and undermine Americans' faith in democracy. That is not just an election cycle threat; it's pretty much a 365-days-a-year threat. And that has absolutely continued.”

While he noted that “enormous strides have been made since 2016 by all different federal agencies, state and local election officials, the social media companies, etc.,” to protect the physical infrastructure of our elections, he said, “I think we recognize that our adversaries are going to keep adapting and upping their game. And so we're very much viewing 2018 as just kind of a dress rehearsal for the big show in 2020.”

Last week, at the House of Representatives, a representative of the Department of Homeland Security also emphasized that Russia and other foreign countries, including China and Iran, conducted influence activities in the 2018 mid-terms and messaging campaigns that targeted the United States to promote their strategic interests.

As you probably know, election administration in the United States is decentralized. It's handled at the state and local levels, so other officials in the United States are charged with protecting the physical infrastructure of our elections, the brick-and-mortar electoral apparatus run by state and local governments, and it is vital that they continue to do so.

However, from my seat on the Federal Election Commission, I work every day with another type of election infrastructure, the foundation of our democracy, the faith that citizens have that they know who's influencing our elections. That faith has been under malicious attack from our foreign foes through disinformation campaigns. That faith has been under assault by the corrupting influence of dark money that may be masking illegal foreign sources. That faith has been besieged by online political advertising from unknown sources. That faith has been damaged through cyber-attacks against political campaigns ill-equipped to defend themselves on their own.

That faith must be restored, but it cannot be restored by Silicon Valley. Rebuilding this part of our elections infrastructure is not something we can leave in the hands of the tech companies, the companies that built the platforms now being abused by our foreign rivals to attack our democracies.

In 2016, fake accounts originating in Russia generated content that was seen by 126 million Americans on Facebook, and another 20 million Americans on Instagram, for a total of 146 million Americans; and there were only 137 million voters in that election.

As recently as 2016, Facebook was accepting payment in rubles for political ads about the United States elections.

As recently as last year, in October 2018, journalists posing as every member of the United States Senate tried to place ads in their names on Facebook. Facebook accepted them all.

Therefore, when the guys on the other panel keep telling us they've got this, we know they don't.

By the way, I also invited Mark Zuckerberg and Jack Dorsey, all those guys, to come and testify at a hearing at my commission when we were talking about Internet disclosure of advertising, and once again, they didn't show up. They didn't even send a surrogate that time; they just sent us written comments, so I feel for you guys.

● (1600)

This is plainly really important to all of us. In the United States, spending on digital political ads went up 260% from 2014 to 2018, from one mid-term election to the next, for a total of $900 million in digital advertising in the 2018 election. That was still less than was spent on broadcast advertising, but obviously digital is the wave of the future when it comes to political advertising.

There have been constructive suggestions and proposals in the United States to try to address this: the honest ads act, which would subject Internet ads to the same rules as broadcast ads; the Disclose Act, which would broaden the transparency and fight against dark money; and at my own agency I've been trying to advance a rule that would improve disclaimers on Internet advertising. All of those efforts so far have been stymied.

Now, we have been actually fortunate that the platforms have tried to do something. They have tried to step up, in part, I'm sure, to try to ward off regulation, but in part to respond to widespread dissatisfaction with the information and the disclosure they were providing. They have been improving, in the United States at least, the way they disclose who's behind their ads, but it's not enough. Questions keep coming up, such as about what triggers the requirement to post the disclaimer.

Can the disclaimers be relied upon to honestly identify the sources of the digital ads? Based on the study about the 100 senators ads, apparently they cannot, not all the time, anyway. Does the identifying information travel with the content when information is forwarded? How are the platforms dealing with the transmission of encrypted information? Peer-to-peer communication represents a burgeoning field for political activity, and it raises a whole new set of potential issues. Whatever measures are adopted today run the serious risk of targeting the problems of the last cycle, not the next one, and we know that our adversaries are constantly upping their game, as I said, and constantly improvising and changing their strategies.

I also have serious concerns about the risks of foreign money creeping into our election system, particularly through corporate sources. This is not a hypothetical concern. We recently closed an enforcement case that involved foreign nationals who managed to funnel $1.3 million into the coffers of a super PAC in the 2016 election. This is just one way that foreign nationals are making their presence and influence felt even at the highest levels of our political campaigns.

These kinds of cases are increasingly common, and these kinds of complaints are increasingly common in the United States. From September 2016 to April 2019, the number of matters before the commission that include alleged violations of the foreign national ban increased from 14 to 40, and there were 32 open matters as of April 1 of this year. This is again an ongoing concern when it comes to foreign influence.

As everything you've heard today demonstrates, serious thought has to be given to the impact of social media on our democracy. Facebook's originating philosophy of “move fast and break things”, cooked up 16 years ago in a college dorm room, has breathtaking consequences when the thing they're breaking could be our democracies themselves.

Facebook, Twitter, Google, these and other technology giants have revolutionized the way we access information and communicate with each other. Social media has the power to foster citizen activism, virally spread disinformation or hate speech and shape political discourse.

Government cannot avoid its responsibility to scrutinize this impact. That's why I so welcome the activities of this committee and appreciate very much everything you're doing, which has carryover effects in my country, even when we can't adopt our own regulations when you all adopt regulations in other countries. Sometimes the platforms maintain the same policies throughout the world, and that helps us. Thank you very much

Also, thank you very much for inviting me to participate in this event. I welcome your questions.

The Chair: Thank you, Ms. Weintraub.

First of all we'll go to Mr. Collins.

Mr. Damian Collins: Thank you. My first question is for Ellen Weintraub.

You mentioned dark money in your opening statement. How concerned are you about the ability of campaigns to use technology, particularly blockchain technology, to launder impermissible donations to campaigns by turning them into multiple, small micro-donations?

● (1605)

Ms. Ellen Weintraub: I'm very concerned about it, in part because our entire system of regulation is based on the assumption that large sums of money are what we need to worry about and that this is where we should focus our regulatory activity. On the Internet, however, sometimes very small amounts of money can be used to have vast impact, and that doesn't even get into the possibility of Bitcoin and other technologies being used to entirely mask where the money is coming from.

So yes, I have deep concerns.

Mr. Damian Collins: Have there been any particular examples that have come to the awareness of your commission?

Ms. Ellen Weintraub: The problem with dark money is that you never really know who is behind it. There has been about a billion dollars in dark money spent on our elections in the last 10 years, and I cannot tell you who is behind it. That's the nature of the darkness.

Mr. Damian Collins: I just wondered whether any particular allegations had been made, or whether there had been cause for any further investigation about what might be considered to be suspicious activity.

Ms. Ellen Weintraub: We have a constant stream of complaints about dark money. The case I just described to you is one of the foremost examples we've seen recently. It can be money that comes in through LLCs or 501(c)(4)s. In this case, it came in through the domestic subsidiary of a foreign corporation.

Mr. Damian Collins: Do you have any concerns about the way technologies like PayPal could be used as well to bring money in from sources trying to hide their identity or even from abroad?

Ms. Ellen Weintraub: PayPal, gift cards and all of those things are deeply concerning. If the money is going directly to a campaign, they can't accept more than a small amount of money without disclosing the source of it, and they're not allowed to accept anonymous contributions above a very small amount of money. However, once you get into the outside spending groups—super PACs and groups like that—they can accept money from corporations, which by definition are a shield against knowing who is really behind them.

Mr. Damian Collins: I'd be interested in the comments of all three of the witnesses in response to my next question.

Ad transparency seems to be one of the most important things we should push for. Certainly in the U.K., and I think in other countries as well, our electoral law was based on understanding who the messenger was. People had to state who was paying for the advert and who the advert was there to promote. Those same rules didn't translate into social media.

Even though the platforms are saying they will require that transparency, it seems, particularly in the case of Facebook, quite easy to game. The person who claims to be the person responsible for the ads may not be the person who is the data controller or the funder. That information isn't really clear.

I wonder if you share our concerns about that, and if you have any thoughts about what sort of legislation we might need to make sure there is full, proper disclosure as to who is funding campaigns.

Ms. Ellen Weintraub: I absolutely share that concern. Part of the problem, as far as I know, is that they're not verifying who is behind the ad. If somebody says Mickey Mouse is the sponsor of this ad, that's what they're going to run on their platform.

Mr. Damian Collins: I'd be interested in hearing from the other two panellists as well, whether they have any concern regarding how we would create a robust system of ad transparency online.

Mr. Daniel Therrien: I would add that to reduce the risk of misuse of information in the political process, you need to have a series of laws. In Canada and a number of other countries, such as the United States, political parties, at least federally in Canada, are not governed by privacy legislation. That's another gap in the laws of certain countries.

You need a series of measures, including transparency in advertising, data protection laws and other rules, to ensure that the ecosystem of companies and political parties is properly governed.

Mr. Damian Collins: It sounds like the heart of it is having regulators who have statutory powers to go into the tech companies and investigate whether they feel the appropriate information is being disclosed.

Mr. Daniel Therrien: We can investigate companies in Canada, but we cannot investigate political parties. A proper regime would authorize a regulator to have oversight over both.

Mr. Damian Collins: That would be both parties and the platforms that are providing the advertising.

Mr. Daniel Therrien: Yes.

Mr. Damian Collins: I don't know if the audio feed to Malta is working.

Prof. Joseph A. Cannataci: The audio feed is working, thank you, Mr. Collins. I thank you also for the work you've put in on your report, which I must say I found to be extremely useful for my mandate.

Very quickly, I share the concerns of both the previous witnesses. The importance of who the messenger was is very, very great when it comes to ad transparency. I share serious concerns about the use of blockchain and other distributed ledger technologies. Frankly, not enough research has been carried out at this moment in time to enable us to examine the issues concerned.

I happen to live in a country that has proclaimed itself the blockchain island, and we have some efforts going on with legislation on blockchain, but I'm afraid there is still a lot of work to be done around the world on this subject. If at all possible, I would suggest that the committee lend its name to some serious resources in studying the problem and coming up with proper recommendations.

● (1610)

The Chair: Thank you, Mr. Cannataci.

We're over time and we have some members who need to go to a vote. Therefore, I need to get to Ms. Vandenbeld as soon as I can.

I will try to get back around if you need a more fulsome answer.

Ms. Vandenbeld.

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

Thank you very much for being here and for your very informative testimony.

I'd like to focus my questions on the foreign threats to democracy and what I call the enabling technologies: the social media platforms, the "data-opolies" that are allowing for those foreign threats to actually take hold.

I note that, as legislators, we are the front lines of democracy globally. If those of us who are elected representatives of the people are not able to tackle this and do something about these threats.... This is really up to us and that's why I'm so pleased that the grand committee is meeting today.

I also note the co-operation that even our committee was able to have with the U.K. committee on AggregateIQ, which was here in Canada when we were studying Cambridge Analytica and Facebook.

However, we do have a problem, which is that individual countries, especially smaller markets, are very easily ignored by these large platforms, because simply, they're so large that individually there is not much we can do. Therefore, we do need to work together.

Ms. Weintraub, do you believe that right now you have the tools you need to ensure that the 2020 U.S. election will be free, or as free as possible, of foreign influence?

Ms. Ellen Weintraub: I hesitate to answer that question. As I said in my testimony, there are various laws that I wish Congress would pass. There are regulations that I wish I could persuade my colleagues on the commission to agree to pass.

I think we are not in as good shape as we could be, but I do know that the Department of Homeland Security and all the state and local governments have been working very hard on ensuring the physical infrastructure, to try to ensure that votes don't get changed, which of course is the biggest fear.

When it comes to foreign influence, as our FBI director said, we are expecting our adversaries to be changing up their game plan, and until we see it, we won't know whether we're ready for it.

Ms. Anita Vandenbeld: In Canada, one of the issues is that during an election campaign it's very hard to know who has the authority to be able to speak out, so we've put together the critical election incident public protocol, which is a group of senior civil servants who would be able to make public if it's known through the security agencies that there is, in fact, a foreign threat.

Has the U.S. looked at something such as that? Is it something that you think would work internationally?

Mr. Cannataci, I would ask you to also answer that in terms of the global context. I wonder if you're seeing things that could potentially, during an election period, allow for that type of authority to be able to speak out on that.

I'll start with Ms. Weintraub and then go to Mr. Cannataci.

Ms. Ellen Weintraub: I do think that authority is there. I think there are federal officials who are empowered to make that type of information public if they become aware of it, as they become aware of it. There are obviously national security and intelligence concerns that sometimes hamper that type of transparency.

Ms. Anita Vandenbeld: Mr. Cannataci, you mentioned that there are international treaties of sorts on data and privacy protection, but is there a clearing house of sorts of international best practice?

We're finding in this committee alone that there are very good examples that we're sharing, but is there any place where these best practices are being shared and tested, and documented and disseminated?

● (1615)

Prof. Joseph A. Cannataci: Not to my knowledge. We have coming up two United Nations committees, at least one of which might be discussing ancillary subjects. There is the so-called open-ended working group inside the UN, which will start working probably in the autumn, where you might be tempted to broach the subject.

I would, however, be pleased to work together with the committee in order to devise any sets of mechanisms that can be shared on good practices, because most of the attempts we have seen in manipulating elections involve profiling individuals in one area or another and then targeting them in order to get their votes.

I'd be very pleased to carry out work, together with the committee, in that direction, and anybody who wishes to share good practices is very welcome to do so.

The Chair: Thank you, Ms. Vandenbeld. That's your time.

We'll go over to Mr. Angus for five minutes.

Mr. Charlie Angus: Thank you, Mr. Chair.

Thank you for appearing, Ms. Weintraub.

You Americans are like our first cousins, and we love you dearly, but we're a little smug, because we look over the border and see all this crazy stuff and say we'd never do that in Canada. I will therefore give you the entire history of electoral fraud and interference in Canada in the last 10 years.

We had a 20-year-old who was working for the Conservatives who got his hands on some phone numbers and sent out wrong information on voting day. He was jailed.

We had a member of this committee who got his cousins to help pay an electoral paying scheme. He lost his seat in Parliament and went to jail.

We had a cabinet minister who cheated on 8,000 dollars' worth of flights in an election and went over the limit. He lost his position in cabinet and lost his seat.

These situations have consequences, and yet we see wide open data interference now for which we don't seem to have any laws, or we're seemingly at a loss and are not sure how to tackle it.

I can tell you that in 2015 I began to see it in the federal election, and it was not noticed at all at the national level. It was intense anti-Muslim, anti-immigrant women material that up-ended the whole election discourse in our region. It was coming from Britain First, an extremist organization. How working-class people in my region were getting this stuff, I didn't understand.

I understand now, however, how fast the poison moves in the system, how easy it is to target individuals, how the profiles and the data profiles of our individual voters can be manipulated.

When the federal government has new electoral protection laws, they may be the greatest laws for the 2015 election, but that was like stage coach robberies compared with what we will see in our upcoming election, which will probably be testing some of the ground for the 2020 election.

In terms of this massive movement in the tools of undermining democratic elections, how do we put in in place the tools to take on these data mercenaries who can target us right down to individual voters each with their own individual fears?

Ms. Ellen Weintraub: I don't even know how to begin to answer that question.

Obviously Canada has a different system from ours in the United States. I don't always agree with the way our Supreme Court interprets the First Amendment, but it has provided extremely strong protections for free speech rights, and that has ramifications in the area of technology, in the area of dark money, in the area of money and politics.

If it were up to me, I think they would veer a little bit more toward the Canadian model, but I don't have control over that.

Mr. Charlie Angus: Mr. Therrien, I will go to you.

It was your predecessor, Elizabeth Denham, who identified the Facebook weakness in 2008 and attempted to have them comply. If they had done so, we might have avoided so many issues. Now, in 2019, we have you making a finding in the rule of law under your jurisdiction that Facebook broke our information protection act.

What has been very disturbing is that Facebook has simply refused to recognize the jurisdiction of our country, based on our supposed necessity to prove to them whether or not harm was caused.

I'm not sure whether you heard Mr. Chan's testimony today, but in terms of the rights of democratic legislators to ensure that laws are protected, how do we address a company that believes it can pick and choose, opt in or opt out, among national laws?

● (1620)

Mr. Daniel Therrien: You refer to the findings of my predecessors 10 years ago. It's certainly disconcerting that practices that were identified 10 years ago and were said to have been corrected by better privacy policies and better information to users were not actually corrected. There were superficial improvements, in our view, but in effect, the privacy protections of Facebook 10 years after the investigation of the OPC are still very ineffective.

On the jurisdictional argument, I believe the argument of the company is that because Canadians were not personally affected in terms of the ultimate misuse of the information for political purposes, this somehow results in the lack of jurisdiction for my office. Actually, however, what we looked at was not limited to the impact of these privacy practices on the Canadian political process. We looked at the sum total of the privacy regulatory scheme of Facebook as it applies not only to one third party application but all third party applications, of which there are millions.

I'm certainly very concerned that Facebook is saying that we do not have jurisdiction, when we were looking at the way in which Facebook handled the personal information of Canadians vis-à-vis millions of applications and not only one application.

How do you ensure that Facebook or other companies heed the jurisdiction of Canada? Well, based on the legal regime that we have, we are left with the possibility of bringing Facebook to the Canadian Federal Court—and this is what we will do—to have a ruling on Facebook's practices, including whether it is subject to our jurisdiction. We don't have much doubt that they are subject to our jurisdiction, but it will take a court finding to decide that question.

Mr. Charlie Angus: Finally—

The Chair: Thank you, Mr. Angus. You're out of time.

Mr. Charlie Angus: My watch says it's four minutes and 53 seconds.

Voices: Oh, oh!

The Chair: We'll have some more time around the hop, so I'd better get going here.

We'll go next to Singapore for five minutes.

Mr. Tong.

Mr. Edwin Tong (Senior Minister of State, Ministry of Law and Ministry of Health, Parliament of Singapore): Thank you.

Ms. Weintraub, thank you very much for being here. In September 2017 you wrote a letter to the then chairman of the FEC. I'll just quote one paragraph from it and ask you some questions. You said, “It is imperative that we update the Federal Election Commission's regulations to ensure that the American people know who is paying for the Internet political communications they see.”

Am I right to assume that your concerns arise from the fact that foreign activity influences, interferes with, and even corrupts political communication, not just in an election but in the everyday life of people in a democratic society, and that if left unchecked over time such activity would seek to undermine institutions and the government, subvert elections and ultimately destroy democracy?

Would I be right to say that?

Ms. Ellen Weintraub: I share many of those concerns and I worry deeply that what is going on is not just election-oriented but is an attempt to sow discord, to sow chaos and to undermine democracy in many countries.

Mr. Edwin Tong: In fact, would you agree that the typical modus operandi of such bad actors would be precisely to sow discord on socially decisive issues; to take up issues that split open fault lines in society so that institutions and ultimately governments are undermined?

● (1625)

Ms. Ellen Weintraub: I believe that is so.

Mr. Edwin Tong: You mentioned earlier the tech companies. I think you said that their answer to you was, “We've got this.” Obviously, that's far from the case. You also said it's obvious that they were not verifying the persons behind the advertisements and the donations.

Are you aware of the Campaign for Accountability, the CFA?

Ms. Ellen Weintraub: I can't say that I am; I'm sorry.

Mr. Edwin Tong: Sometime, I think, after you released Robert Mueller's findings, a non-profit organization called Campaign for Accountability posed as IRA operators, bought political ads and did so very easily. They were able to effectively get Google to run a whole series of advertisements and campaigns for a little less than $100 U.S. and they managed to get something like 20,000 views and more than 200 clicks with that kind of spending.

Is that something that would concern you, and should regulations deal with that kind of obvious foreign activity that also shows that media platforms cannot be trusted to police?

Ms. Ellen Weintraub: I absolutely think there is a need for greater regulation to ensure that when people see things on social media, they can trust where it's coming from.

Mr. Edwin Tong: Yes.

On the regulations that you spoke of, from the quote that I read to you, could you maybe, in 30 seconds, tell us what you think should be the core principles behind such regulations to stop the influence and corruption of foreign interference in democratic processes?

Ms. Ellen Weintraub: Well, as I said, I think what we need is greater transparency. When people are reading something online, they need to be able to know where it's coming from.

We had this example of ads and information being placed, propaganda, coming from the Internet Research Agency in Russia. I don't know anybody who wants to get their news from a Russian troll farm. I think if they knew that was where it was coming from, that would tell them something about how much to believe it.

Mr. Edwin Tong: Yes, because ultimately, false information is not free speech, is it?

Ms. Ellen Weintraub: People need to know where the information is coming from, and then they can draw better conclusions.

Mr. Edwin Tong: Yes. Thank you.

Thank you, Mr. Chair.

The Chair: Thank you.

We'll go next to Ms. Naughton from Ireland.

Ms. Hildegarde Naughton (Chair, Joint Committee on Communications, Climate Action and Environment, Houses of the Oireachtas): My first question will be for Mr. Cannataci. It's in relation to legislation we're looking at in Ireland, which could ultimately apply at a European level. It's an online digital safety commissioner. One of the key challenges our committee is having in relation to drawing this legislation is the definition about what is harmful communication. I don't know if you could assist us. Is there a best practice or best way of going about that?

We're also legislating ultimately at a European level, and as we know, we need to protect freedom of speech and freedom of expression. Those issues have been raised here. Have you any comments to make in relation to that?

Prof. Joseph A. Cannataci: The short answer is, yes, I would be happy to assist you. We are setting up a task force precisely on privacy and children and online harm. It's a very difficult subject, especially because some of the terminology that has been used is not very clear, including the use of words such as “age appropriate”.

For most kids around the world, there's no such thing as one age being associated with a given level of maturity. Kids develop at different ages. The type of harm that they can receive really needs to be better studied. In fact, there are very few studies, unfortunately, on this subject. There are some studies, but not enough.

I would certainly welcome a joint European, Irish, and indeed, international approach on the subject, because this is something that goes across borders, so thank you for that.

Ms. Hildegarde Naughton: Thank you very much. I think that's a common concern here around the table in relation to that definition.

I might ask the Privacy Commissioner, Mr. Therrien, in relation to GDPR, do you have any viewpoints on how that's working?

As you know, Facebook's Mark Zuckerberg has called for GDPR to be rolled out on a global level. I'd like your own comments, from your own professional background.

It is quite new. As you know, it has been rolled out at a European level. What are your viewpoints on that, how it's working, and Mr. Zuckerberg's call for that to be rolled out, even on a modified level, from country to country?

● (1630)

Mr. Daniel Therrien: The GDPR is still relatively new, so in terms of how it is working, I think we'll need to wait a bit longer to see what its impact is in practice. I certainly believe that the principles of the GDPR are good ones; they're good practices. I believe that individual countries obviously should seek to have the most effective privacy and data protection possible and borrow from other jurisdictions rules that have that impact.

In my opening statement, I mentioned interoperability. In addition, it's important that the national laws, although interoperable and borrowing from good principles such as the GDPR, are also aligned and informed by the culture and traditions of each country. There might be differences in certain jurisdictions, say, on the various weight or the relative weight of freedom of expression versus data protection, but GDPR is an excellent starting point.

Ms. Hildegarde Naughton: Okay, thank you.

I think those are my questions.

The Chair: You have one minute.

Ms. Hildegarde Naughton: Do you want to ask a question?

Mr. James Lawless (Member, Joint Committee on Communications, Climate Action and Environment, Houses of the Oireachtas): Thanks.

Chair, if it's okay, I'll just use the last minute, but I'll come in on the second round again for my five minutes.

The Chair: Yes, you bet.

Mr. James Lawless: Ms. Weintraub, it was interesting to listen to your analysis of what happened in the recent elections, and I suppose particularly of nation-states' influence.

One thing that I think is common is that it's not necessarily that they favour one candidate over another, but—it seems to be a common theme—that they favour dissent and, I suppose, weakening western democracies. I think we saw that arguably in Brexit as well as in the U.S. elections. How do we combat that?

I have drafted legislation similar to the honest ads act, the social media transparency act, with very similar objectives. One question, and I'll come back to it in the second round, is about how we actually enforce that type of legislation. Is the onus on the publishers or is it on the platform?

We heard somebody mention that they had successfully run fake ads from the 100 U.S. senators or members of the House of Representatives or whatever it was. Should it be the platforms that are liable for ensuring that the correct disclosure and disclaimers and verification are performed? They say back to us that they can't possibly do that. Do we, then, make the people who are running the ads liable, or do we make the people who are taking out the ads liable, if you understand the distinction?

Ms. Ellen Weintraub: Historically what we do in the States is put the onus on whoever is placing the ads to make sure that their disclaimers and disclosure obligations are fulfilled. It seems to me, though, that we could take advantage of the vaunted machine learning AI capabilities of these platforms. If the machines can detect that the name on the ad bears no relation at all to the source of the payment, you would think they could have a human being take a look at it and say, "Hey, let's just make sure we have the right name here on the ad."

It's not the way our laws work right now, though.

The Chair: Next up for five minutes is Mr. Zimmermann from Germany.

Mr. Jens Zimmermann (Social Democratic Party, Parliament of the Federal Republic of Germany): Thank you, Mr. Chair.

I would first start with Mr. Cannataci and would focus on international co-operation.

We brought up earlier here that on an international level, co-operation is needed. This is also the idea behind our meeting here. Where, though, do you see forums for co-operation in these areas? We'll have, for example, the Internet Governance Forum, which is a multi-stakeholder approach on the UN level, this year in Germany.

Do you see any other approaches?

● (1635)

Prof. Joseph A. Cannataci: Thank you for that question, Mr. Zimmermann.

The Internet Governance Forum is a useful place to meet and talk, but we must be very careful not to let it remain just a talking show. The problem is that it is a forum in which many interesting ideas are heard but very little governance takes place. At this moment in time, the states unfortunately tend to dodge the responsibility of providing actual governance.

I think what we're going to see, and I think the companies feel this coming—some of them have half-admitted it—is countries getting together, including the European Parliament that has just been elected, and increasingly using measures that will focus attention.

Nothing focuses attention like money. The GDPR approach, which has been referred to, has companies around the world paying close attention, because nobody wants to be stuck with a bill of 4% of their global turnover. I think that this is one measure that will help introduce liability and responsibility. To come to the previous question, I think it will also focus attention on platforms at least as much as publishers, because as somebody said, sometimes it's difficult to detect whether the publisher was the right person.

Mr. Jens Zimmermann: Thank you very much.

The enforcement question would have been my follow-up, but you already answered. Thank you.

I would also ask Ms. Weintraub one question.

We have mentioned many times now trolls and troll farms, and we're focusing very much on advertisements. What about home-grown trolls? We've seen to a certain degree also in Germany that especially on the far right there are activists who are really trolls on steroids. You don't have to pay them; they do this because they want to support their political affiliates.

They're also using tools whereby, in the dark, they decide to focus on such-and-such member of Parliament, attacking him or her, or simply supporting every post done by a member of a party. They are simply making the most out of the algorithms, and they don't need any money for it

Do you have that also on the radar?

Ms. Ellen Weintraub: I think you raise another very serious question. We have seen this in the States, that some of the techniques that were pioneered by foreign activists are now being adopted by domestic activists because they've seen that they work. It has the same kind of concerning effect as promoting discord, and hate speech sometimes, and gathering from the crevices of the community people who have views that in isolation might not have much power but that, when they are able to find each other online and promote these ideas, become much more concerning.

We don't have good tools to go after that, because it's easy to say, if it's foreigners, that they're trying to intervene in our election, and we know that's not a good thing. When it's our own people, though, it's a bigger challenge.

The Chair: You have about 30 seconds.

Mr. Jens Zimmermann: I'll raise maybe one last aspect.

We have a lot of regulation of the media, what is allowed for a TV station, for a radio station, but in Germany right now we have a lot of debate about YouTube, people who basically have more of an audience than many TV stations but are not regulated at all.

Is that something you are also seeing?

Ms. Ellen Weintraub: We certainly have the phenomenon of influencers. I don't spend a lot of time on YouTube myself, and when I see some of these folks, I'm really not sure why they have this kind of influence and sway, but they do.

It goes back to the model that we have. The model of regulation in the United States is a money-based model. When we began to address political activity on the Internet, it was at a point when YouTube was in its infancy and the governing assumption was that of course somebody would have to pay to put these ads up in order for anybody to see them. Now we're dealing in a whole different world in which all this free content is up there and it goes viral. There are very few controls on that.

● (1640)

The Chair: Thank you.

We're going to get back to our parliamentarians, now that they've returned from voting.

We'll go to Mr. Kent for five minutes.

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

My first question is for Commissioner Therrien and is related to the revelation in the government's response to an Order Paper question regarding discriminatory advertising for employment, on a number of platforms, it seems, but certainly Facebook was mentioned, in which a number of departments had requested micro-targeting advertising by sex and age.

Mr. Chan, the CEO of Facebook Canada, responded that yes, that was the case but protocols have changed, although there was a certain imprecision or ambiguity in his responses. He said that the Government of Canada has been advised that it is not only unacceptable but quite possibly illegal under various human rights legislation across the country.

Could I have your response, Commissioner?

Mr. Daniel Therrien: I think this shows the importance of having regulations that are human rights based. Here we have a practice that allegedly resulted or could result in discrimination. I think it's important that the regulations look at the net effect of a practice and deal with it from a human rights perspective.

In terms of privacy, we tend to look at privacy or data protection as rules around consent and specification of purpose and so forth. I think Cambridge Analytica raised the issue of the close relationship between privacy protection, data protection and the exercise of fundamental rights, including, in the case of your example, equality rights.

I think that for the types of laws for which I'm responsible in Canada, by defining privacy not with regard to important mechanisms such as consent, for instance, but with regard to the fundamental rights that are protected by privacy, we would have a more effective and more fulsome protection.

Hon. Peter Kent: Okay.

The question for you, Ms. Weintraub, is on the discussion we had with Facebook this morning with regard to the Pelosi altered video and the statement that Facebook made to the Washington Post saying,“We don't have a policy that...the information you post on Facebook must be true.”

Clearly, this is a case of political maliciousness. It is not an election year, but certainly it is tainting the well of democracy and obviously targeting one political leader's reputation and political leadership. I'm wondering what your thoughts are with regard to the Facebook argument.

They will take down a video by someone posting the truth who is falsely posting, but they will leave up the video placed by someone who is obviously quite willing to say that they put the video up and simply to put an advisory that it doesn't seem to be the truth, even though, in the Pelosi case, that manipulated video has been seen by many millions of viewers since the controversy developed, which again feeds the business plan of Facebook with regard to clicks and number of views.

Ms. Ellen Weintraub: Well, I heard a lot of dissatisfaction voiced this morning about the answer that Facebook gave. I have to say that I also found their answer to be somewhat unsatisfactory, but it raises a really important question. I mean, in this case they know it's not true, but the broader question is, who is going to be the arbiter of truth?

Personally, I don't want that responsibility, and I think it's dangerous when government takes on that responsibility of deciding what is true and what isn't. That really veers more into the Orwellian, more authoritarian governance. I don't think I would feel comfortable either being that person or living in a regime where government had that power, but if government doesn't have that power, then the question is, who does? I'm also uncomfortable with the platforms having that much power over determining what is truth and what isn't.

● (1645)

Hon. Peter Kent: If that were to occur in an election cycle, what would your response be?

Ms. Ellen Weintraub: In election cycles, we have various regulations that govern ads, if indeed it is paid advertising and if it mentions candidate names. Every member of the House of Representatives runs every two years. I suppose that for a member of the House of Representatives they are always in cycle, but we have stronger rules that govern once we get closer to the election. Within 30 days of a primary or 60 days of a general election, there are rules, again, that go to disclosure, though. We don't have any rules that would empower my agency to order a platform to take down an ad.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Ms. Weintraub.

Some of the membership of the committee are not going to ask questions, so we have a bit more time than you might expect. If you do want to ask another question, please signal the chair, and I'll add you in at the end of the sequence.

Next up, we have the member from Estonia.

Go ahead.

Ms. Keit Pentus-Rosimannus (Vice-Chairwoman, Reform Party, Parliament of the Republic of Estonia (Riigikogu)): Thank you.

Ms. Weintraub, I have a question for you.

Disinformation is officially part of Russia's military doctrine. It has been so for some time already. They are using it as a strategy to divide the west, basically. It is also known that Russia uses 1.1 billion euros per year for their propaganda and spreading their narratives.

Your next presidential elections are practically tomorrow. Knowing the things we now know about the last campaigning period, are you ready today? If what happened during the previous campaign would reappear, and if all the same things would happen again, do you think that now you would be able to solve it?

Ms. Ellen Weintraub: I'm not going to claim that I can personally solve the problem of disinformation in our elections. As I mentioned earlier, I think there are laws and regulations that have been drafted and should be adopted that would strengthen our position.

I also think that we, writ large, need to devote more attention to digital literacy. A lot of people believe all sorts of things that they see online and that they really shouldn't. My daughter tells me that this is generational, that her generation is much more skeptical of what they read online and that it's only my foolish generation that views the Internet as this novelty and assumes that everything they read is true.

I don't know that I entirely agree that it's entirely a generational problem, but I do think that we, as a whole, as the broader community of democracies, really need to look into what our resiliency is to the kind of disinformation that we know is going to be out there.

As I said, we're always fighting the last battle, so we can write laws to address what happened last time, but I'm quite sure that in the next election new techniques are going to be developed that nobody's even thinking about yet.

Ms. Keit Pentus-Rosimannus: Can you say what are the two main threats you are preparing for?

Ms. Ellen Weintraub: My agency is all about regulating money in politics. That is our focus, so we are trying to look at where the money is coming from. That is what we're always looking at. We're trying to get better transparency measures in place so that our voters and our electorate will better know where the money is coming from and who is trying to influence them. That's really my number one priority.

Ms. Keit Pentus-Rosimannus: We just had elections in Europe, the European parliamentary elections. Do you see anything we went through that could be used to prepare for your next election? How closely do you co-operate with European colleagues?

Ms. Ellen Weintraub: I'm always happy to get information from any source. That's why I'm here. It's a very educational event for me. As well, I'm happy to answer any questions that you all may have.

● (1650)

Ms. Keit Pentus-Rosimannus: Do you see already that there are some things from the European Parliament elections that you can find useful?

Ms. Ellen Weintraub: We have not yet studied what went on in the European Parliament elections.

Ms. Keit Pentus-Rosimannus: All right.

The Chair: You're good? Thank you.

We're going to start the cycle again, just so you know. We'll start with Nate, and then we'll go to the next parliamentarian, so it will be Nate, Ian and James.

Go ahead, Nate.

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

I was in Brussels recently and met with the EU data protection supervisor. There is great co-operation among the privacy commissioners in the EU. There are conferences for privacy commissioners where you get together and discuss these issues as a matter of co-operation amongst regulators.

Is there the same level of co-operation, Ms. Weintraub, with respect to elections?

Ms. Ellen Weintraub: Our elections are run under our own unique rules. As I said before, I'm happy to have information from any source, but because our rules are different from other countries' rules, particularly when it comes to the transparency of money and politics and how we fund our elections, we kind of plow our own course.

Mr. Nathaniel Erskine-Smith: When I suggested to a friend from Colorado and a friend from Mississippi that I wanted to get involved in politics and said that the cap in my local district was $100,000 Canadian, they laughed at me for a long time.

Voices: Oh, oh!

Ms. Ellen Weintraub: It's very different.

Mr. Nathaniel Erskine-Smith: Before I move to Mr. Therrien, I completely respect that as an American you have stronger free speech rules than we have here in Canada. Still, when you say "arbiters of truth", there are still standards councils and there are still, when it comes to broadcasters.... Surely, a broadcaster in an election.... Maybe I'm incorrect, but I would expect that there are standards councils and some ethics guidelines and some basic principles they would abide by, and they wouldn't just broadcast anything.

Ms. Ellen Weintraub: I think that's true of broadcasters, mostly out of a sense of professional responsibility. That is one of the conundrums that I think we all face. When we were living in a world where there was a small number of broadcasters and those were all professional journalists, and they had training and they exercised editorial control over what they were distributing and were doing a lot of fact-checking, that was a whole different world from the information that we get online, where everybody's a broadcaster, everyone is a content producer, and—

Mr. Nathaniel Erskine-Smith: So sort of, right...? Because it's one thing for you and me to be friends on Facebook and you post something and I see it. It's a very different thing if the News Feed, the algorithm that Facebook employs, makes sure I see it because of a past history that I have online, or if the YouTube recommendation function ensures that I see a video that I wouldn't see otherwise because I didn't seek it out. Aren't they very akin to a broadcaster when they're employing algorithms to make sure I see something and they're increasing impressions and reach?

Ms. Ellen Weintraub: You're discussing an entirely different topic. I was talking about individuals who are putting their own content out there. The way the platforms are regulated under current United States law is that they don't have those same responsibilities as broadcasters under section 230 that—

Mr. Nathaniel Erskine-Smith: If they took their corporate social responsibility seriously, as broadcasters do, presumably they would join a standards council or create one.

With respect to ad transparency, we recommended at this committee.... I mean, the honest ads act would be a good start, but I think it would just be a first step.

Ms. Ellen Weintraub: Absolutely.

Mr. Nathaniel Erskine-Smith: Does it make sense to you that if I'm receiving an ad online, especially in an election, that I would be able to click through and see who paid for it, obviously, but also the demographics for which I've been targeted, as well as a selection criteria on the back end that the advertiser has selected, whether it's Facebook or Google or whatever it might be, for example, if it has been directed to a particular postal code, or if it's because I'm between the ages of 25 and 35? Do you agree that there should be more detailed transparency?

Ms. Ellen Weintraub: I do, but of course part of the problem with that, though, is that very few people would actually click through to find that information. One concern I have is that everybody says that as long as you can click through and find the information somewhere, that should be good enough. I think there has to be some information right on the face of the ad that tells you where it's coming from.

● (1655)

Mr. Nathaniel Erskine-Smith: Right.

The last question I have is for Mr. Therrien.

We had a number of excellent witnesses last night and this morning who really highlighted the business model as the fundamental problem here, in that it encourages this never-ending accumulation of data.

I wonder if you have any comments on two ideas that I want to set out. One, how do we address that business model problem that was identified? Two, how do we address it in such a way that it also respects the real value of aggregate-level data in different ways?

If I look at Statistics Canada, for example, which publishes aggregate-level data, that is really helpful for informed public policy. When I use Google Maps on a daily basis, that is based upon user information that is fed into the system and, as a result, I don't need to know where I'm going all the time; I can use Google Maps. It's based on data that has been input, but in the public interest.

How do we address the business model but also protect the public interest use of aggregate-level data?

Mr. Daniel Therrien: I think an important part of the solution is to look at the purposes for which information is collected and used. It's one thing for an organization, a company, to collect and use data to provide a direct service to an individual. That is totally legitimate, and this is the type of practice that should be allowed. It's another for an organization to collect so much information, perhaps under the guise of some type of consent, that the end outcome is something very close to corporate surveillance.

I think it's important to distinguish between the two. There are a number of technical rules that are at play, but the idea that we should define privacy beyond mechanical issues like consent and so on and so forth and define it by regard to what is the right being protected, i.e., the freedom to engage in the digital economy without fear of being surveilled, is an important part of the solution.

Mr. Nathaniel Erskine-Smith: I'm out of time, but I'll just say one final thing. When you think of privacy from a consumer protection perspective, it's a curious thing that when I buy a phone I don't have to read the terms and conditions. I know that if it's a defective phone I can take it back, because there are implied warranties that protect me, but for every app I use on my phone, in order to be protected, I have to read the terms and conditions. I think it's just a crazy thing.

Thanks very much.

The Chair: Thank you, Mr. Erskine-Smith.

I want to speak to the order of questions. This is what I have: Ian, James, David de Burgh Graham, Jo, Jacques, Charlie and Peter. To close out, we have Mr. Collins again, for some final words. That's what we have so far. If there is anybody else who wants to ask a question, please put your hand up. I'll try to get you added to that list, but it looks like we're tight for time.

Now we're going to Mr. Lucas for five minutes.

Mr. Ian Lucas (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you, Mr. Chairman.

I was very struck by something that Jim Balsillie said this morning. He said that the online business model of the platforms "subverts choice", and choice is what democracy is essentially about. It occurred to me—you might find this quite amusing—that in the United Kingdom, broadcasters aren't allowed to do political advertising. In other words, we don't have the wonderful advertisements that I've seen in the United States, and I'm sure in other jurisdictions.

Do you think there's a case for banning paid-for political advertising online on these platforms?

Ms. Ellen Weintraub: I don't see any way it would pass constitutional scrutiny on our Supreme Court.

Mr. Ian Lucas: That's in the United States?

Ms. Ellen Weintraub: Yes. It's my frame of reference.

Mr. Ian Lucas: Yes.

If I can talk to you, Mr. Cannataci, is the use of political advertising through broadcasting worldwide nowadays? Are there jurisdictions where broadcast advertisements are not accepted?

Prof. Joseph A. Cannataci: Thank you for the question, Mr. Lucas.

The answer is that national practices vary. Some countries go more towards the United States model. Others go towards the United Kingdom model. In truth, though, we are finding that in many countries where the law is more restrictive, in practice many individuals and political parties are using social media to get around the law in a way that was not properly envisaged in some of the actual legislation.

With the chair's permission, I'd like to take the opportunity, since I've been asked a question, to refer to something that I think is transversal across all the issues we have here. It goes back to the statement made by Ms. Weintraub regarding who is going to be the arbiter of truth. In a number of countries, that value is still very close to our hearts. It is a fundamental human right, which happens to reside in the same article 17 of the International Covenant on Civil and Political Rights, of which many of the countries around the table, if not all, are members.

In the same section that talks about privacy, we have the provision on reputation, and people [*Technical difficulty—Editor*] care a lot about their reputation. So in terms of the arbiter of truth, essentially, in many countries, including France—I believe there was some discussion in Canada too—people are looking at having an arbiter of truth. Call him the Internet commissioner or call him the Internet ombudsman, call him what you will, but in reality people want a remedy, and the remedy is that you want to go to somebody who is going to take things down if something is not true.

We have to remember—and this applies also to online harm, including radicalization—that a lot of the harm that is done on the Internet is done in the first 48 hours of publication, so timely takedown is the key practical remedy. Also, in many cases, while freedom of speech should be respected, privacy and reputation are best respected by timely takedown. Then, if the arbiter in the jurisdiction concerned deems that it was unfair to take something down, it can go back up. Otherwise, we need the remedy.

Thank you.

● (1700)

Mr. Ian Lucas: It occurs to me, going back to Mr. Erskine-Smith's point, that when I joined Facebook I didn't consent to agree to be targeted by political advertising from anywhere. I didn't know that was part of the deal. It's not why people join Facebook.

It seems to me that we've managed, give or take a few bad phases, to survive as a democracy in the U.K. without broadcast TV adverts, political adverts. It's a particular area of advertising that I'm seeking to restrict, and I'm supported because of the emphasis that was given this morning to the way the control of data is really removing choice from the individual in this process.

From an information regulation point of view, how clear do you think people are in that area? Do you think people understand that this is what's happening here?

Ms. Ellen Weintraub: First of all, let me say that I think there are many people in the United States who would love a system where they didn't get political advertisements. It's not something that people actually enjoy all that much.

I think you're raising a nuance there that I think is important, and that is, it's not.... Our Supreme Court would never allow a sort of a flat-out ban on political advertising, but—

Mr. Ian Lucas: Right. It's the position of the United States, but—

Ms. Ellen Weintraub: Right, but what you're talking about is the use of people's personal data to micro-target them, and that, it seems to me, does raise a very different issue. I'm not actually sure that it wouldn't pass constitutional scrutiny.

Mr. Ian Lucas: That's exactly what's happening in terms of paid-for advertising at the moment.

The other issue—

The Chair: Mr. Lucas, could you could make it real quick? I hate to cut you off. You've come a long way.

Mr. Ian Lucas: Very quickly, I'll pick up on an issue that Jens mentioned. He talked about trolls. Closed groups are also a massive problem, in that we do not have the information, and I think we need to concentrate more on that as an issue, too.

The Chair: Thank you, Mr. Lucas.

Next up, we have James from Ireland.

Mr. James Lawless: Thank you, Chair. I have another couple of questions and observations.

Just picking up on something that I think Nate was saying earlier in his other points, the question often is whether these platforms are legally publishers or dumb hosts, terminals that display the content that gets put in front of them. I think one argument to support the fact that they're publishers and therefore have greater legal responsibilities is that they have moderators and moderation policies, with people making live decisions about what should and shouldn't be shown. On top of that, of course, are the targeting algorithms. I think that's something that's of interest, just as an observation.

On my other point, before I get into questions, we were talking about nation-states and different hostile acts. One thing that's the topic of the moment, I suppose, is the most recent revelation in terms of the Chinese government and the Huawei ban, and the fact that Google, I think in the last few days, announced a ban on supporting Huawei handsets. But it strikes me that Google is tracking us through Google Maps and everything else as we walk about with our phones. I think I read that there are 72 million different data points in a typical year consumed just by walking about town with a phone in your hand or in your pocket. Maybe the difference is that somewhere Google has terms and conditions that we're supposed to take, and Huawei doesn't, but both are effectively doing the same thing, allegedly. That's just a thought.

On the legislative framework, again, as I mentioned earlier, I've been trying to draft some legislation and track some of this, and I came to the honest ads act. One of the issues we've come across, and one of the challenges, is balancing free speech with, I suppose, voter protection and protecting our democracies. I'm always loath to criminalize certain behaviours, but I'm wondering what the tipping point is.

I suppose that in the way I've drafted it initially what I've considered is that I think you can post whatever you whatever you want as long as you're transparent about who actually said it, who is behind it, who is running it or who is paying for it, particularly if it's a commercial, if it's a paid-for post. In terms of the bots and the fake accounts, and what I would call the industrial-scale fake accounts, where we have a bot farm or where we have multiple hundreds or thousands of users actually being manipulated by maybe a single user or single entity for their own ends, I think that probably strays into the criminal space.

That's one question for Ms. Weintraub.

I suppose another question, a related question, is something that we struggle with in Ireland and that I guess many jurisdictions might struggle with. Who is responsible for policing these areas? Is it an electoral commission? If so, does that electoral commission have its own powers of enforcement and powers of investigation? Do you have law enforcement resources available to you? Is it the plain and simple police force of the state? Is a data protection commissioner in the mix as well? We have different types of regulators, but it can be a bit of an alphabet soup, and it can be difficult to actually pin down who is in charge. Also, then, if we do have somebody in charge, it can be difficult; they don't always have the resources to follow through.

That's my first question. In terms of criminalization, is that a bridge too far? Where do you draw the line? Second, if there is criminalization and there's an investigation required, what kind of resourcing do you have or do you think is needed?

● (1705)

Ms. Ellen Weintraub: Again, my expertise is in the U.S. system, so I can most effectively tell you about that. We are a law enforcement agency. We have jurisdiction over money and politics, and we have civil enforcement authority. We have subpoena authority. We can do investigations. I think that some of our enforcement tools could be strengthened, but we also have the ability to refer to our justice department if we think there are criminal violations, which are basically knowing and wilful violations of the law.

Going back to something that you said earlier, in terms of our regulatory system, I don't think bots have first amendment rights. They're not people, so I don't have any problem with.... I don't understand why these smart tech companies can't detect the bots and get them off the platforms. I don't think that would raise first amendment concerns, because they're not people.

Mr. James Lawless: Actually, that's a great line. I'm going to use that again myself.

I think I still have time for my next question. There is another way around this that we've seen in Ireland and, I guess, around the world. We've heard it again today. Because of the avalanche of fake news and disinformation, there is a greater onus on supporting the—dare I say—traditional platforms, the news media, what we'd call independents, quality news media.

There is a difficulty in terms of who decides what's independent and what's quality, but one of the approaches that we've been looking at I think I heard it in the Canadian Parliament when we watched the question period a few hours ago. I heard similar debates. One solution we're toying with is the idea of giving state subsidies or state sponsorship to independent media, not to any particular news organization but maybe to a broadcasting committee or a fund that is available to indigenous current affairs coverage, independent coverage.

That could be online, or in the broadcast media, or in the print media. It's a way to promote and sustain the traditional fourth estate and the traditional checks and balances of democracy but in a way that I suppose has integrity and is supported, asks questions of us all, and acts as a foil to the fake news that's doing the rounds. However, it's a difficult one to get right, because who decides who's worthy of sponsorship and subsidy and who isn't? I guess if you can present as a bona fide, legitimate local platform, you should be entitled to it. That's an approach we're exploring, one that has worked elsewhere and has seemed to work in other jurisdictions.

● (1710)

The Chair: Thank you James.

Next we'll go to Mr. Graham.

Go ahead for five minutes.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Thank you.

Ms. Weintraub, to build on that, if bots don't have first amendment rights, why does money?

Ms. Ellen Weintraub: Well, money doesn't have first amendment rights. It's the people who are spending the money who have first amendment rights.

Let me be clear about this. I'm not a big fan of our Supreme Court jurisprudence. I mean, I would adopt the Canadian jurisprudence on this stuff if I could, but it's a little bit above my pay grade.

Mr. David de Burgh Graham: Fair enough. So you don't necessarily think the decision in Citizens United was a good one?

Ms. Ellen Weintraub: It would be fair to say that I am not a fan of the Citizens United decision.

Mr. David de Burgh Graham: Fair enough.

As you were saying, the elections commission's job is to oversee the financing of elections. If a company knowingly permits the use of its algorithm or platform to influence the outcome of an election, would you consider that to be a regulated non-monetary contribution?

Ms. Ellen Weintraub: I think it could be an in-kind contribution.

Mr. David de Burgh Graham: Interesting. My next question is related to that.

The CEO of Facebook has a majority of voting shares in the company. He basically has absolute powers in that company. From a legal or regulatory point of view, what prevents that company from deciding to support or act in any way they feel like in an election?

Ms. Ellen Weintraub: As a corporation, it can't give a donation directly to a candidate, and that would include an in-kind contribution.

A question was raised earlier—and forgive me as I can't recall if it was you who suggested it—about Mark Zuckerberg running for president and using all of the information that Facebook has accumulated to support his campaign. That would be a massive campaign finance violation because he doesn't own that information. Facebook, the corporation, owns it.

The wrinkle in that is that due to the decision of our Supreme Court, corporations can make contributions to super PACs, which supposedly act independently of the campaigns. If a super PAC were advancing the interests of a particular candidate, a corporation—including Facebook—could make an unlimited contribution to that super PAC to help them with their advocacy.

Mr. David de Burgh Graham: Understood.

I don't have much time, so I'll go to Mr. Therrien for a quick second.

To Mr. Lucas's point earlier, in the social media world, are we the client or are we the product?

Mr. Daniel Therrien: It is often said that when you do not pay with money, you are the product, and there is certainly a lot of truth to that phrase.

Mr. David de Burgh Graham: When a surveillance-based company adds tags to sites that do not belong to them, with the approval of the site owner—for example, Google Analytics is pervasive across the Internet and has the approval of the site owner but not of the end user—do you consider them to have implied consent to collect that data?

Mr. Daniel Therrien: Sorry, I did not get the end.

Mr. David de Burgh Graham: If I have website and have Google Analytics on it, I have approved Google's use of my website to collect data, but somebody coming to use my website doesn't know that Google is collecting data on my site. Is there implied consent, or is that illegal from your point of view?

Mr. Daniel Therrien: It is one of the flaws of consent, probably, that there is a term and condition somewhere that makes this consent. That's why I say that privacy is not only about the rules of consent; it's about the use of the information and the respect for rights. We should not be fixated on consent as the be-all and end-all of privacy and data protection.

The Chair: We have Mr. Picard, who will share the rest of the time with—

Mr. Michel Picard (Montarville, Lib.): Ms. Weintraub, you said something very interesting, and I don't know whether we have established this notion before.

In the scenario where Zuckerberg would run for president, Facebook couldn't give the information because it would be a massive contribution in kind. Have we established the ownership of the information? No one has consented that this information be spread, and therefore does Facebook own this information?

● (1715)

Ms. Ellen Weintraub: That is a very interesting question, but I'm not sure it's a campaign finance question, so it may be outside of my expertise.

Mr. Michel Picard: What if it were in Canada, Mr. Therrien?

Mr. Daniel Therrien: The rules around ownership of information are not very clear.

From a privacy and data protection perspective, I think the question is one of control, consent, but ownership is not a clearly cut question in Canada.

The Chair: Thank you.

The last three are Jo, Jacques, Charlie, and then we'll finish up.

Ms. Jo Stevens (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you, Chair.

Ms. Weintraub, I want to ask you, as someone with an obvious professional interest and expertise in this area, do you think we in the U.K. would have more confidence in the integrity in our elections and referenda if we had a Mueller-type inquiry into the 2016 European Union referendum?

Ms. Ellen Weintraub: You know your people better than I do. I think you're a better judge of what would give them greater confidence.

There were specific incidents that triggered the Mueller inquiry.

Ms. Jo Stevens: Do you see any overlap between those incidents, or any trend in terms of what happened there and what you know about the European Union referendum?

Ms. Ellen Weintraub: I haven't studied it carefully enough to wage an opinion.

Ms. Jo Stevens: Okay, thank you.

In terms of the future for us, we potentially have a second referendum coming up soon. We may have another vote. We may even have a general election very shortly.

Are there any recommendations you would make, in terms of foreign interference through money to the U.K. and to our government? At the moment, our electoral laws, I think, are generally accepted to be unfit for purpose in the digital age.

Ms. Ellen Weintraub: As I said, I think a lot of it goes to transparency. Do you have the ability to know who is behind the information that you're seeing both digitally and in other media?

Ms. Jo Stevens: Are there any jurisdictions that you would identify currently as having really good electoral laws that are fit for purpose, bearing in mind what we've all been talking about today around digital interference? Is there a country that you would hold up as a really good model?

Ms. Ellen Weintraub: I keep looking for that. I go to international conferences, and I'm hoping that somebody out there has the perfect solution. However, I have to say that I haven't found it yet.

If you find it, let me know, because I would love to find that country that's figured this out.

Ms. Jo Stevens: Perhaps I could ask Mr. Cannataci the same question.

Is there a jurisdiction you're aware of that you think we could all look to for best practice on electoral law encompassing the digital age?

Prof. Joseph A. Cannataci: The short answer is no.

I share Ms. Weintraub's problem. I keep looking for the perfect solution and I only find, at best, half-baked attempts.

Ms. Stevens, we'll stay in touch about the matter, and the minute we find something, I'll be very happy to share it.

Ms. Jo Stevens: Thank you.

The Chair: You have two minutes, Jo.

Ms. Jo Stevens: That's good.

The Chair: Okay.

Next up, we have Monsieur Gourde.

Go ahead, for five minutes.

[*Translation*]

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

My question will focus on a word that seemed to me to be important just now, the word “responsibility”.

This morning, we heard from representatives from digital platforms. They seemed to brush away a major part of their responsibility.

That shocked me. I feel they have a responsibility for their platforms and for the services they provide. Despite very specific questions, they were not able to prove that they are in control of their platforms in terms of broadcasting fake news or hate propaganda that can really change the course of things and influence a huge number of people.

The users, those that buy advertising, also have a responsibility. When you buy advertising, it must be fair and accurate, in election campaigns especially, but also all the time.

If there was international regulation one day, how should we determine the responsibility of both parties, the digital platforms and the users, so they can be properly identified?

That question goes to anyone who wants to answer.

● (1720)

Mr. Daniel Therrien: In terms of protecting data or privacy, you have put your finger on concepts that are fundamental, in my opinion; they are responsibility and accountability. We live in a world where there is massive information gathering and where the information is used by companies for a number of purposes other than the first purpose for which they had been obtained.

The companies often tell us that the consent model is not effective in protecting the privacy of the public, the consumers. They are partly right. Their suggestion is to replace consent, when it is ineffective, by increased accountability for the companies. I feel that that proposal must come with a real demonstration that companies are responsible and they cannot simply claim to be. That is why it is important for regulatory organizations to ensure that companies are really responsible.

[*English*]

Ms. Ellen Weintraub: It seems to me that they are occupying a sort of hybrid space. They say they're not broadcasters. They say they're just the platform and they're not responsible for any of the content, yet they do seem to feel that they have some responsibility, because they are taking steps. People may feel the steps are inadequate, but they are taking some steps to provide greater transparency.

Why are they doing that? I think it's because they know they can't quite get away with just ignoring this entire issue. They do bear some responsibility in a broader sense, if not in a particular legal sense in any particular jurisdiction. Whether they would have stronger responsibilities if particular jurisdictions, either on an individual basis or on a global basis, decided to say, “No, no, you really are broadcasters and you have to start acting like it”, that is a question for legislators, not regulators.

[*Translation*]

Mr. Jacques Gourde: Is there, anywhere in the world…

Mr. Cannataci, did you want to add a comment?

Prof. Joseph A. Cannataci: Yes. Thank you.

I certainly share Mr. Therrien's opinion, but I would like to add something else.

[*English*]

If I could in this questioning just pick out one thing, it is to say that for whoever is going to control whether something should be taken down or not, or whether it's true or not—whatever—it requires effort, and that requires resources. Resources need to be paid for, and who is collecting the money? It's largely the companies.

Of course, you can have somebody for whom you can genuinely say, “Okay, this was the party, or the sponsor, or whoever who paid for the ad.” Otherwise, when push comes to shove, I think we're going to see a growing argument and a growing agreement in a lot of jurisdictions, which will say that they think the companies are collecting the money and, therefore, they have the means to control things. We've seen that to be the case when, for example, Facebook needed to have people who spoke the language of Myanmar in order to control hate speech in that country. I think we're going to see an increasing lead in many national jurisdictions and potentially probably international agreements attributing accountability, responsibility and fiscal liability for what goes on the platforms to the people who collect the money, which is normally the platforms themselves, to a large extent.

Thank you, Mr. Chair.

The Chair: Thank you.

We'll go to you, Mr. Angus, for five minutes, with Mr. Collins following you, and then me.

Mr. Charlie Angus: Thank you, Mr. Chair.

We heard an extraordinary statement from Google today that they voluntarily stopped spying on our emails in 2017. They did that in such a magnanimous manner, but they wouldn't agree not to spy on us in the future because there may be nifty things they can do with it.

I can't even remember 2016—it's so long ago—but 2018 changed our lives forever. I remember our committee was looking at consent and whether the consent thing should be clear or it should be bigger with less gobbledygook.

I don't ever remember giving Google consent to spy on my emails or my underage daughters' emails. I don't ever remember that it came up on my phone that, if I wanted to put my tracking location on so I could find an address, they could permanently follow me wherever I went and knew whatever I did. I don't remember giving Google or any search engine the consent to track every single thing I do. Yet, as legislators, I think we've been suckered—Zuckered and suckered—while we all talked about what consent was, what consumers can opt in on, and if you don't like the service, don't use it.

Mr. Therrien, you said something very profound the last time you were here about the right of citizens to live free of surveillance. To me, this is where we need to bring this discussion. I think this discussion of consent is so 2016, and I think we have to say that they have no consent to obtain this. If there's no reason, they can't have it, and that should be the business model that we move forward on: the protection of privacy and the protection of our rights.

As for opt-in, opt-out, I couldn't trust them on anything on this.

We've heard from Mr. Balsillie, Ms. Zuboff, and a number of experts today and yesterday. Is it possible in Canada, with our little country of 30 million people, to put in a clear law that says you can't gather personal information unless there's an express, clear reason? It seems to me that's part of what's already in PIPEDA, our information privacy laws, but can we make it very clear with very clear financial consequences for companies that ignore that? Can we make decisions on behalf of our citizens and our private rights?

● (1725)

Mr. Daniel Therrien: Of course the answer to that is yes. I think there is a role for consent in certain circumstances where the relationship is bilateral between a company service provider and a consumer, where the consumer understands the information that is required to provide the service. With the current digital economy, we're way beyond that. There are many purposes for which the information is then used, often with the purported consent of the consumer.

While there is a place for consent, it has its limits, and that's why I say it is important that privacy legislation define privacy for what it is. It is not at all limited to the mechanical question of consent. It is a fundamental right linked to other fundamental rights. When the outcome of a practice of a company, despite purported consent, is to surveil a consumer in terms of data localization or in terms of the content of messages given by that person, then I think the law should say that consent or no consent, it doesn't matter. What is at play is a privacy violation, being the surveillance of the individual in question, and that is a violation per se that should lead to significant penalties. It is possible to do that.

Mr. Charlie Angus: Thank you.

My final question is on facial recognition technology. There's a story in the Toronto Star today that the police are using facial recognition technology. San Francisco has attempted to ban it, and other jurisdictions are at least putting a pause on it.

As for the right of a citizen to be able to walk in a public square without being surveilled and without having to bring photo ID, facial recognition technology changes all that. There are obviously legitimate uses. For example, if someone on a CCTV camera has committed a crime, and there's a database, we would maybe have judicial oversight that this is a fair use; however, what about a number of people in a crowd that you can just gather in? I'm sure Facebook and Google would be more than helpful because they have such massive facial recognition databases on us.

As a Canadian regulator, do you believe that we need to hit a pause button on facial recognition technology? How do we put the rules in place to protect citizens' rights with clear safeguards for police use and for commercial use prior to abuses?

● (1730)

Mr. Daniel Therrien: I think in terms of moratoria or outright prohibitions, I would distinguish between the use of a technology—the technology of facial recognition—and the uses to which the technology is put. I find it more likely that a ban or a moratorium would make sense for specific uses of a technology than for the technology per se, because for facial recognition there might be useful public purposes including in a law enforcement domain where, despite the privacy restrictions of facial recognition, the overall public good is in favour of using the technology. I would look at it in terms, again, of specific uses for technology. In that regard, yes, it would make sense to prohibit certain uses.

The Chair: Thank you, Mr. Angus.

Last, Mr. Collins, go ahead.

Mr. Damian Collins: Thank you very much.

Ellen Weintraub, given what we've talked about this afternoon, dark money in politics and how difficult it is to have any kind of proper oversight of what happens on platforms like Facebook, are you frightened by the news reporting that Facebook is going to launch its own cryptocurrency?

Ms. Ellen Weintraub: Yes.

Mr. Damian Collins: You are. You're frightened by the prospect.

I think you're right to be frightened by the prospect. Given all the other problems we've talked about, this seems like a sort of political money launderer's charter.

Do you not think people will look back on this period of time and say we had sophisticated democracies and societies that have developed decades of rules and regulations on campaign finance, electoral law, personal rights about data and privacy, oversight of broadcast media and news and other forms of news as well, and that we were prepared to see all those decades of experience bypassed by a company like Facebook, simply because that's the way their business model works, and it's unsustainable, the position that we're in at the moment?

Ms. Ellen Weintraub: Whether it's unsustainable, whether it requires further regulation, I think is exactly why all of you are sitting around this table today.

Mr. Damian Collins: But in some ways, listening to the discussion in this last session, we're tying ourselves in knots trying to solve a problem that's being caused by a company. Actually it may well be that the solution is, rather than having to abandon lots of things that we value because they've been put there to protect citizens and citizens' rights, we actually should say to these companies, “This is what we expect of you, and we will force this upon you if we can't be convinced there's any other way of doing it”, and we're not prepared to tolerate people being exposed to dark hats, elections being interfered with by bad actors, disinformation, hate speech spreading uncontrolled, and actually, these are not the standards we expect in a decent society. We say that recognizing that platforms like Facebook have become the main media channel in terms of how people get news and information, anywhere between a third and a half of Europeans and Americans.

Ms. Ellen Weintraub: I think there is a real risk trying to take a set of rules that evolved in the 20th century and assuming that they're going to be equally appropriate for the technologies of the 21st century.

Mr. Damian Collins: The final comment from me is that I think that's right. Those rules have been demonstrated to be out of date because of new technology and the way people engage with content in the world. Surely, what should remain is the values that brought in those rules in the first place. Saying that those rules need to change because technology's changed is one thing. What we shouldn't say is that we should abandon those values simply because they've become harder to enforce.

Ms. Ellen Weintraub: I absolutely agree with that.

The Chair: Mr. Therrien.

Mr. Daniel Therrien: I totally agree.

The Chair: I would like to finish up with one thing. We've been talking about the subpoena to Mark Zuckerberg and Sheryl Sandberg for some time and, as chair of this committee, I will say we did our very best to make sure they attended today. We're limited by what's in this book and the laws of our country, and yet the platforms seem to operate in their own bubbles without any restriction within our jurisdictions, and that's the frustration for us as legislators in this place.

Again, thank you for appearing today and thank you for assisting us, especially Commissioner Therrien, for your work in assisting this committee. We look forward to keeping those conversations going in the future.

I have some housekeeping aspects of what's going to happen tonight. Dinner is going to be at 7 p.m., downstairs in room 035. This is room 225, so two floors down will be where dinner is. It's at 7 p.m.

Just to be clear, each delegation is to give a brief presentation on what your country has done and is looking at doing to fix this problem. I'll be talking with my vice-chairs about how we're going to deliver what we are doing in Canada, but I challenge you to have that ready. Again, it's going to be brief. It can be informal. It doesn't need to be a big written presentation. I see some very serious looks on faces wondering, “What did we just get ourselves into?”

More important, I see a lot of tired faces. I think we're all ready just to go back to the hotel for about an hour's rest and then we'll reconvene at 7 p.m. I think that's all I have to say for now, but again we'll see you back at 7 p.m.

● (1735)

Mr. Charlie Angus: I have a point of order, Mr. Chair, before you try to shut us all down.

I do want to commend the excellent work of the staff, our analysts who have put this together, and Mr. Collins for what was done in England. This goes above and beyond. I think we have really set a standard. I'm hoping that in the next Parliament, and maybe in other jurisdictions, we can maintain this conversation. You've done incredible work on this. We really commend you for it.

[*Applause*]

The Chair: Thank you for that. For the record, we will be holding the other platforms to account tomorrow morning at 8:30.

We'll see you tonight at seven o'clock.