HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 152 • 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

● (0830)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): We're calling to order meeting 152 of the Standing Committee on Access to Information, Privacy and Ethics. Today in Ottawa, we have the international grand committee on big data, privacy and democracy.

I'm going to go over the countries quickly. We're not going to go through introductions because it would take up too much time, unfortunately.

We have the United Kingdom. With me today is Damian Collins, the co-chair of the international grand committee. He'll make comments in a few minutes.

We have the Parliament of Singapore with us. The Houses of the Oireachtas are here from Ireland. The Parliament of the Federal Republic of Germany is with us. The Chamber of Deputies of the Republic of Chile is with us. The Parliament of the Republic of Estonia is here. The Senate of the United Mexican States is with us. The House of Representatives of the Kingdom of Morocco is with us. We have the National Assembly of the Republic of Ecuador. The Legislative Assembly of the Republic of Costa Rica is here. Finally, the House of Assembly of Saint Lucia is with us.

I want to introduce my co-chair, Mr. Damian Collins.

Welcome.

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

It's a pleasure to be with you here in Ottawa.

It's great to see that since the first meeting of the grand committee in London in November we have new members of the committee here today with additional countries represented. I think it just shows how these issues are only growing in significance. I'm sure today's discussions will add greatly to that debate.

The Chair: Absolutely. Thank you, Mr. Collins.

We'll start off with our witnesses this morning.

As individuals, we have Mr. Jim Balsillie, chair, Centre for International Governance Innovation; Mr. Roger McNamee, author of *Zucked*; Shoshana Zuboff, author of *The Age of Surveillance Capitalism*; and last but certainly not least, from Manila in the Philippines, we have Maria Ressa, chief executive officer and executive editor of Rappler Inc.

Today, we'll start off with our very own, Jim Balsillie.

Go ahead.

Mr. Jim Balsillie (Chair, Centre for International Governance Innovation, As an Individual): Thank you.

Co-chairs Zimmer and Collins and committee members, it's my honour and privilege to testify today.

Data governance is the most important public policy issue of our time. It is cross-cutting, with economic, social and security dimensions. It requires both national policy frameworks and international coordination.

Over the past three years, Mr. Zimmer, Mr. Angus and Mr. Erskine-Smith have spearheaded a Canadian bipartisan effort to deal with data governance. I'm inspired by the seriousness and integrity they bring to the task.

My perspective is that of a capitalist and global tech entrepreneur for 30 years and counting. I'm the retired chairman and co-CEO of Research in Motion, a Canadian technology company that we scaled from an idea to $20 billion in sales. While most are familiar with the iconic BlackBerry smartphone, ours was actually a platform business that connected tens of millions of users to thousands of consumer and enterprise applications via some 600 cellular carriers in more than 150 countries. We understood how to leverage Metcalfe's law of network effects to create a category-defining company, so I'm deeply familiar with multi-sided, platform business model strategies, as well as with navigating the interface between business and public policy.

I'll start with several observations about the nature, scale and breadth of our collective challenge here.

Disinformation and fake news are just two of the many negative outcomes from unregulated attention-based business models. They cannot be addressed in isolation. They have to be tackled horizontally as part of an integrated whole. To agonize over social media's role in the proliferation of online hate, conspiracy theories, politically motivated misinformation and harassment is to miss the root and scale of the problem.

Second, social media's toxicity is not a bug—it's a feature. Technology works exactly as designed. Technology products, services and networks are not built in a vacuum. Usage patterns drive product development decisions. Behavioural scientists involved with today's platforms help design user experiences that capitalize on negative reactions, because they produce far more engagement than positive reactions.

Third, among the many valuable insights provided by whistleblowers inside the tech industry is this quotation: “The dynamics of the attention economy are structurally set up to undermine the human will”. Democracy and markets work when people can make choices aligned with their interests. The online advertisement-driven business model subverts choice and represents a foundational threat to markets, election integrity and democracy itself.

Fourth, technology gets its power through control of data. Data at the micro-personal level gives technology unprecedented power to influence. Data is not the new oil. It's the new plutonium—amazingly powerful, dangerous when it spreads, difficult to clean up and with serious consequences when improperly used. Data deployed through next generation 5G networks is transforming passive infrastructure into veritable digital nervous systems.

Our current domestic and global institutions, rules and regulatory frameworks are not designed to deal with any of these emerging challenges. Because cyberspace knows no natural borders, digital transformation's effects cannot be hermetically sealed within national boundaries. International coordination is critical.

With these observations in mind, here are my six recommendations for your consideration.

One, eliminate tax deductibility of specific categories of online ads.

Two, ban personalized online advertising for elections.

Three, implement strict data governance regulations for political parties.

Four, provide effective whistle-blower protections.

Five, add explicit personal liability alongside corporate responsibility to affect CEO and board of director decision-making.

Six, create a new institution for like-minded nations to address digital co-operation and stability.

Technology is disrupting governance and, if left unchecked, could render liberal democracy obsolete. By displacing the print and broadcast media in influencing public opinion, technology is becoming the new fourth estate. In our system of checks and balances, this makes technology coequal with the executive, the legislative bodies and the judiciary.

When this new fourth estate declines to appear before this committee, as Silicon Valley executives are currently doing, it is symbolically asserting this aspirational coequal status, but is asserting this status and claiming its privileges without the traditions, disciplines, legitimacy or transparency that check the power of the traditional fourth estate.

● (0835)

The work of this international grand committee is a vital first step towards redress of this untenable current situation. As Professor Zuboff said last night, we Canadians are currently in a historic battle for the future of our democracy with a charade called Sidewalk Toronto.

I'm here to tell you that we will win that battle.

Thank you.

The Chair: Thank you, Mr. Balsillie.

Next up, for five minutes we'll go to Mr. McNamee.

Mr. Roger McNamee (As an Individual): Co-Chairs Zimmer and Collins, members of the committee, thank you for the opportunity to address you today. My remarks will build on last night's presentations by Professor Zuboff, Professor Tworek, Ben Scott and today's by Jim.

For the 35 years I spent as an investor, I shared Silicon Valley's commitment to technology that empowers the people who use it. Beginning in 2004, however, I noticed a transformation in the culture of Silicon Valley, and over the course of a decade, customer-focused models were replaced by the relentless pursuit of global-scale monopoly and massive wealth.

As Professor Zuboff told you, Google was the first to see the economic opportunity from converting all human experience into data. Google wants to make the world more efficient. They want to eliminate user stress that results from too many choices. Now, Google knew that society would not permit a business model based on denying consumer choice and free will, so they covered their tracks. Beginning around 2012, Facebook adopted a similar strategy, later followed by Amazon, Microsoft and others.

For Google and Facebook, the business is behavioural prediction. They build a high-resolution data avatar of every consumer—a voodoo doll, if you will. They gather a tiny amount of data from user posts and queries, but the vast majority of their data comes from surveillance: web tracking, scanning emails and documents, data from apps and third parties, and ambient surveillance from such products as Alexa, Google Assistant, Sidewalk Labs and Pokémon GO.

Google and Facebook use data voodoo dolls to provide their customers, who are marketers, with perfect information about every consumer. They use the same data to manipulate consumer choices. Just as in China, behavioural manipulation is the goal.

The algorithms of Google and Facebook are tuned to keep users on site and active, preferably by pressing emotional buttons that reveal each user's true self. For most users, this means content that provokes fear or outrage. Hate speech, disinformation and conspiracy theories are catnip for these algorithms. The design of these platforms treats all content precisely the same, whether it be hard news from a reliable site, a warning about an emergency or a conspiracy theory. The platforms make no judgments: users choose, aided by algorithms that reinforce past behaviour. The result is 2.5 billion Truman Shows on Facebook, each a unique world with its own facts.

In the U.S., nearly 40% of the population identifies with at least one thing that is demonstrably false. This undermines democracy. The people at Google and Facebook are not evil. They are products of an American business culture with few rules, wherein misbehaviour seldom results in punishment. Smart people take what they can get and tell themselves they've earned it. They feel entitled. Consequences are someone else's problem.

Unlike industrial businesses, Internet platforms are highly adaptable, and this is the challenge. If you take away one opportunity, they will move on to the next one, and they are moving upmarket, getting rid of the middleman. Today they apply behavioural prediction to advertising, but they have already set their sights on transportation and financial services.

This is not an argument against undermining their advertising business, but rather a warning that it may be a Pyrrhic victory. If your goals are to protect democracy and personal liberty, you have to be bold. You have to force a radical transformation of the business model of Internet platforms. That would mean, at a minimum, banning web tracking, scanning of email and documents, third party commerce and data, and ambient surveillance. A second option would be to tax micro-targeted advertising to make it economically unattractive.

You also need to create space for alternative business models, using anti-trust law. Start-ups can happen anywhere. They can come from each of your countries.

● (0840)

At the end of the day, though, the most effective path to reform would be to shut down the platforms at least temporarily, as Sri Lanka did. Any country can go first. The platforms have left you no choice. The time has come to call their bluff. Companies with responsible business models will emerge overnight to fill the void.

Thank you very much.

● (0845)

The Chair: Thank you, Mr. McNamee.

We'll go next to Ms. Zuboff.

Ms. Shoshana Zuboff (As an Individual): Thank you, co-chairmen Zimmer and Collins. It's such a pleasure to be here today.

As you know, I hail from the Harvard Business School, where I am a professor emerita. More importantly, I am the author of this book on surveillance capitalism. I say that because I want you to know that any statements and conclusions I reach today are amply supported by the information and analysis in that work. I might add that my scholarly work on the digital future began in the year 1978. I'll let you do the math on that.

My remarks this morning cover some highlights of a longer written statement that I have submitted to the committee. I add for the record that I am deeply committed to the work of this very important group. That includes continuing to support your work in any way I can, off-line or in future meetings, as we engage in this world-historic challenge.

The Internet is now an essential medium of social participation, and it is owned and operated by private surveillance capital. The questions of law and regulation that this committee seeks to explore cannot be answered without a clear grasp of surveillance capitalism as a novel economic logic defined by distinct economic imperatives that compel specific practices. I don't want to repeat everything that I talked about last night. Roger has touched on some of the key issues, as has Jim, so I will skip ahead to the idea of economic imperatives.

What we see in surveillance capitalism is the unilateral claiming of private human experience, its translation into behavioural data and their fabrication into prediction products, which are sold in a new kind of marketplace that trades exclusively in human futures. When we deconstruct the competitive dynamics of these markets, we get to understand what the new imperatives are. First of all, it's scale. They need a lot of data in order to make good predictions; economies of scale. Secondly, it's scope. They need varieties of data to make good predictions. Ultimately, in the third phase of this competitive struggle, it was discovered that the most predictive data comes from actually intervening in human behaviour, intervening in the state of play, in order to have predictions that come closer and closer to actual observations so that they can guarantee outcomes to their business customers. That is how you win in human futures markets.

I'll share with you one brief quote from a data scientist that rings in everybody's ears when they hear it. He said to me, “We can engineer the context around a particular behaviour and force change that way.... We are learning how to write the music, and then we let the music make them dance.”

Friends, this is behavioural modification, systemically institutionalized on a global scale, mediated by a now-ubiquitous digital infrastructure. It began online. It travelled off-line into the real world on our telephones, our cellphones, and ultimately now we live in a world of devices, which allows this to be amplified and perpetuated. This digital architecture is growing every day. I call it the “big other”. It is at this new level of competitive intensity that it is no longer enough to automate information flows about us. The goal now is to automate us. The goal is to automate us not only as individuals, not only as small groups, but increasingly also on the scale of populations. The goal is to have surveillance capitalism's computational analysis that favours its own commercial outcomes replace democracy and governance as we know it.

In fact, at this very moment in the city of Toronto, Alphabet-owned Sidewalk Labs is spinning its own new euphemisms, which it calls “governance innovation”. This is Orwellian code for the deconstruction of local democracy in favour of Sidewalk's computational rule, which is, in the final analysis, a reincarnation of a kind of absolutist tyranny that we thought we had left behind us in the 18th century, now served with cappuccino and draped in ones and zeroes.

● (0850)

Surveillance capitalism assaults democracy from below and from above. From below, it is a direct assault on human autonomy and agency essential for the possibility of a democratic society. From above, it is marked by asymmetries of knowledge and power the likes of which human history has never seen.

I want to move on to the question of what is to be done, because this is what we really didn't have time to discuss very much last night, and build on Jim's excellent, excellent recommendations, all of which I agree with.

Surveillance capitalism has thrived in the absence of law, as we all know. I take that as a positive sign, because what this means is that we have not failed to rein in this rogue mutation of capitalism. The real issue is that we haven't really tried. The accompanying good news is that our societies have experience in reining in the raw excesses of a destructive capitalism. We did it to end the Gilded Age. We did it to mitigate the Great Depression. We did it in the post-war era. We did it in the seventies to save creatures, air, water, workers and consumers. We know how to do this. This is what democracy is for. It is time to do it again.

The great business historian Tom McCraw wrote a brilliant history of regulation in the 20th century, the 19th and 20th centuries. He identified several phases of regulatory regimes, starting in the late 19th century with the muckrakers and moving into the early 20th century with the progressives. Later, in the New Deal and in the early 1970s, the regulatory frameworks were run by legal minds, legal scholars and legal experts. Finally, by the late 1970s, the eighties and right down to today, it's the economists who have held sway.

But this has been a changing dynamic, and what he notes is that at the end of the day, when you look at the more than a century of regulatory issues and regulatory frameworks, the emphasis has come down on fairness and justice over narrow considerations of economic growth. McCraw asks this question: The economists' hour will not last; what is it that will come next?

I want to tell you what it is that will come next. The next great regulatory vision will be framed and implemented by you and by us. It will be elected officials, citizens and specialists, allied in the knowledge that, despite its failures and shortcomings, democracy is the one idea to emerge from the long human story that enshrines the people's right to self-governance and asserts the ideal of the sovereign individual, which is the single most powerful bulwark against tyranny. We give up these ideas at our peril, but only democracy can impose the people's interests through law and regulation.

McCraw also warns that regulators have failed when they did not adequately frame strategies appropriate to the particular industries that they were regulating. The question is, what kind of law and regulation today will be 21st-century solutions aimed at the unique 21st-century complexities of surveillance capitalism?

There are three arenas in which legislative and regulatory strategies can effectively align with the structure and consequences of surveillance capitalism.

Briefly, first, we need lawmakers to devise strategies that interrupt and in many cases outlaw surveillance capitalism's foundational mechanisms. This includes the unilateral taking of private human experience as a free source of raw material and its translation into data. It includes the extreme information asymmetries necessary for predicting human behaviour. It includes the manufacture of computational prediction products, based on the unilateral and secret capture of human experience. It includes the operation of prediction markets that trade in human futures.

● (0855)

Second, from the point of view of supply and demand, surveillance capitalism can be understood as a market failure. Every piece of research over the last decades has shown that when users are informed of the backstage operations of surveillance capitalism, they want no part of it. They want protection. They reject it. They want alternatives.

We need laws and regulatory frameworks designed to advantage companies that want to break with the surveillance capitalist paradigm. Forging an alternative trajectory to the digital future will require alliances of new competitors who can summon and institutionalize an alternative ecosystem. True competitors who align themselves with the actual needs of people and the norms of market democracy are likely to attract just about every person on earth as their customers.

Third, lawmakers will need to support new forms of citizen action —collective action—just as, nearly a century ago, workers won legal protection for their rights to organize, to bargain and to strike. New forms of citizen solidarity are already emerging in municipalities that seek an alternative to the Google-owned smart city future, in communities that want to resist the social costs of so-called "disruption" imposed for the sake of others' gain, and among workers who seek fair wages and reasonable security in the precarious conditions of the so-called gig economy.

Citizens need your help but you need citizens, because ultimately they will be the wind behind your wings. They will be the sea change in public opinion and public awareness that supports your political initiatives. If, together, we aim to shift the trajectory of the digital future back toward its emancipatory promise, we resurrect the possibility that the future can be a place that all of us might call home.

Thank you.

The Chair: Thank you, Ms. Zuboff, for that testimony.

We'll go next to Ms. Ressa, for 10 minutes.

Ms. Maria Ressa (Chief Executive Officer and Executive Editor, Rappler Inc., As an Individual): Co-chairmen Zimmer and Collins, I'm still in the same clothes. Good evening from Manila.

As I said early in our morning—your night last night—we here in the Philippines are a cautionary tale for you, an example of how quickly democracy crumbles and is eroded from within and how these information operations can take over the entire ecosystem and transform lies into facts. If you can make people believe that lies are facts, you can control them. Without facts, you don't have truth. Without truth, you don't have trust.

Journalists have long been the gatekeepers for facts. When we come under attack, democracy is under attack. When this situation happens, the voice with the loudest megaphone wins.

The Philippines is a petri dish for social media. As of January 2019, as We Are Social and Hootsuite have said, Filipinos spend the most time online and the most time on social media globally.

Facebook is our Internet, but as I'll show you with some of the data—you should get them handed to you—this is about introducing a virus into our information ecosystem. Over time, that virus lies, masquerading as facts. That virus takes over the body politic and you need to develop a vaccine. That's what we're in search of, and I think we do see a solution.

I've been a journalist for more than 30 years. My book, published in 2011, *From Bin Laden to Facebook*, looked at how this transformation, this virulent ideology of terrorism, moved from the physical world to the virtual world, and how the al Qaeda-linked group, the Abu Sayyaf here in the Philippines, actually in 2011 used YouTube to try to negotiate ransoms for the people it kidnapped.

I first began looking at social networks in this spread of the virulent ideology. While writing the book, I stumbled on the strategy for Rappler, the start-up that we created in 2012. Using social media and journalism—we embraced it, I drank the Kool-Aid—we built communities of action in a country with weak institutions and endemic corruption. If social networks are your family and friends in the physical world, social media is your family and friends on steroids—no boundaries of time and space.

Understanding information cascades was essential to the growth of Rappler. We were alpha partners of Facebook. We believed and made real social media for social change, and we grew by 100% to 300% year-on-year from the time we were founded in 2012 to 2015. Then, like in the rest of the world, 2016 happened. In May of 2016, President Duterte was elected. A month later, there was Brexit and so on and so on. That was a tipping point for the information operations in our system.

In the Philippines, the weaponization of social media began in July 2016, after President Duterte won—not coincidentally when our brutal drug war began. In a global study with 12 other research groups, we helped define patriotic trolling: online state-sponsored hate meant to pound you into silence, to incite hate against the target and to stifle dissent or criticism. One of the first targets of attack was journalists and newsgroups.

I'm going to quickly show you here the astroturfing that's typical of a three-pronged attack on a target in the Philippines.

The first step is to allege corruption. It doesn't have to be true. Just allege it. If you do it exponentially, it becomes truth. A lie told a million times is truth. Step two, for a woman, if you're a female, you will get attacked sexually. Step three is to lay the groundwork for what you want to happen, whatever that policy is.

In this case, the propaganda machine tried to trend—if you can zoom in here on what I'm showing you, hopefully you'll get this—#ArrestMariaRessa. From there, it went on to jump from the government's creator, the blogger, to a Twitter account that was used in the campaign, so whatever was used in the campaigns then became weaponized. In Tagalog, it says, [*Witness spoke in Tagalog*], "Call her to the Senate #ArrestMariaRessa." Then it moves to "I can smell an arrest and possible closure of Rappler.com". Then finally it moves to the sexual attacks: "Maybe Maria Ressa's dream is to become the ultimate porn star in a gangbang scene"—it is not.

● (0900)

Then finally—and this is a real person who just graduated from college—“Me to the RP government, make sure Maria Ressa gets publicly raped to death when martial law expands to Luzon. It would bring joy in my heart.” #ArrestMariaRessa was an attempt to trend this, to astroturf it. This was in May 2015. My first arrest was in February 2019.

When I was arrested...the methodology is all too familiar. You astroturf on social media, you jump laterally to co-opted traditional media, then repeat and pound top down. In the case of the attack against me and Rappler, it came from President Duterte himself during his state of the nation address in July 2017.

Social media, in 2016, began to lay down the foundation of the legal cases that were filed against us. Starting in January 2018, the government filed 11 cases and investigations against me and Rappler in a 14-month period—roughly a case a month. In about three months, I posted bail eight times. In a five-week period, I was arrested twice and detained once. My only crime is to be a journalist, to speak truth to power, to defend the press freedom that is guaranteed under our constitution.

Here's how it happened. Let me show you.

This is a database that we actually began to put together as a defence. Since we lived on social media, we were able to identify the attacks early on. We found a sock puppet network of 26 fake accounts. As journalists, we then did due diligence to make sure it was fake, and then we went and counted manually. How many accounts could it impact? From 26 fake accounts, they could impact as many as three million.

That became the basis of this database. This is over time, from January 2015 all the way to April 2017. You can basically see the same thing that's happened in the west, which is that there is a fracture line of society, and then, after the drug war began, it was pounded, literally pounded a million times, and it becomes fact. It becomes a solid line.

After this, *bayaran*—it translates to corrupt—was pounded so frequently that it had 1.7 million comments in a one-month period.

I want to show you the database and the very crude UX that we built for our social media team, because it shows you how the information ecosystem is interrelated. This one shows you the URLs that are controlled, or can be, by Google or YouTube. In the middle rung here, you'll see the Facebook pages that actually spread that URL. Then here, you'll see the average reposting time.

What we did for our team so they could find the difference between information operations and a real person was to actually show, after we published the propaganda series in October 2016.... When it's red, that means it's been reposted more than 10 times. We zoomed in on one account, and you can see that this is actually just the same post reposted over and over again, not just on websites but also on Facebook pages that were used in the campaign, not just that of President Duterte but also that of vice-presidential candidate Bongbong Marcos.

So what do we do? Here's the last thing I want to show you. This is data, which, when you look at it this way, actually doesn't show you much. It's just a list of Facebook pages, and then the weighted degree—in degree, out degree, and then a weighted degree. But, if you put it together, you will see this network. This is the social network that was behind the attack on our vice-president, Leni Robredo, in 2017. I think it's because these same.... It was so organized and it has been sustained. We're talking about almost three years that we've lived through this. The content creators are broken down by demographic. This account—this is where the attack began—takes care of the pseudo-intellectual, the supposed thinking class.

● (0905)

Next is the middle-class content creator in this account, and then we have the mass base account. From there it jumps to traditional media, but the co-opted one is the newspaper and, essentially, the chairman emeritus is the man in charge of international public relations for President Duterte. From there, it connects with state media, and then you close the link on this entire group.

By the way, at that point in time, in 2017, the Philippines and Russia inked a partnership, and we actually had state media employees in Sputnik's offices.

Finally, you close it by taking that mass base account and appointing her to head social media for the presidential palace. It's an incredible ecosystem.

Where does this go and what can we do about it? In the long term, it's education. You've heard from our other three witnesses before me about exactly some of the things that can be done. In the medium term, yes, there is media literacy, but in the short term, frankly, it's only the social media platforms that can do something immediately. We're on the front lines. We need immediate help and immediate solutions.

Rappler is one of three fact-checking partners of Facebook in the Philippines, and we do take that responsibility seriously. We don't look at the content alone. Once we check to make sure that it is a lie, we look at the network that spreads the lie. The first step is to stop a new virus from entering the ecosystem. It is whack-a-mole if you look only at the content, but when you begin to look at the networks that spread it, then you have something that you can pull out.

The Chair: Ms. Ressa, could we have you close off your testimony? We're at 12 minutes. I'd like to get to questions if we could.

● (0910)

Ms. Maria Ressa: Sure.

To end with this, I don't know...unless you've been the subject of an attack.... It's very difficult to go through 90 hate messages per hour, sustained over days and months. That is what we're going through, that kind of astroturfing that turns lies into truth. For us, this is a matter of survival.

The Chair: My apologies for cutting you off. Your testimony is powerful, and we have watched your story from afar.

We'll get to questions.

I will have to warn you that we're only going to have enough time for one question per delegation in this particular round. In the next round, we have enough time for everybody.

We're going to start off with Damian Collins, then go to Nathaniel Erskine-Smith, Peter Kent and Mr. Angus, and then go through the delegation. That should give us five minutes each. Again, it's going to be tight. I'm going to try to keep us on a five-minute timeline as much as I possibly can.

We'll start with Mr. Collins.

Go ahead.

Mr. Damian Collins: Thank you, Mr. Chair.

Is that five minutes per delegation?

The Chair: Yes, that's correct.

Mr. Damian Collins: I have two short questions and hopefully my colleagues will be able to get in.

Roger McNamee, in your book, you said, "As far as I can tell, Zuck has always believed that users value privacy more than they should." On that basis, do you think that we are going to have to establish in law the standards we want to see enforced in terms of users' rights and data privacy, with independent regulators to oversee them? Because the companies will never do that effectively themselves. They just don't share the concerns we have about how the systems are being abused.

Mr. Roger McNamee: Yes, I believe that not only is that correct in terms of their philosophy, but as Professor Zuboff points out, it is baked into their business model. It is this notion that any data that exists in the world, claimed or otherwise, they will claim for their own economic use.

Again, framing how you do that privacy is extremely difficult and, in my opinion, would be best done by simply banning the behaviours that are used to gather the data.

Mr. Damian Collins: This is the final question for me.

You also suggest in your book that the problems in terms of election interference could have started around the time that certain advertising tools, such as lookalike audiences, were launched on the platform. I'd be interested to hear if you have anything more to say about that.

Also, do you believe that some of these targeting tools—as I think Professor Zuboff suggested as well—should be banned from digital advertising? Maybe you shouldn't be able to use lookalike audiences. Indeed, in the U.K., the information commissioner has already questioned whether they're legal under GDPR.

Mr. Roger McNamee: Essentially, the problem here is the inversion of politics from the advocacy of a set of policies, and convincing people to join you on those policies, to an election where the number of campaigns is equal to the number of voters and you can use the micro-targeting to take these campaigns to the individual level.

In the United States, it was used to suppress the vote. I can't speak to exactly how it was done in Brexit, but it's very obvious there was a dramatic effect there.

The essential point here is whether you believe that one can have a healthy democracy in an environment where there is advertising that's completely unaccountable because the only people who see it are the intended recipients.

Mr. Damian Collins: Thank you.

I'll cede the rest of my time.

The Chair: It's two and a half minutes.

Mr. Ian Lucas (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): I was very interested, Mr. Balsillie, in what you were saying about creating a structure of holding the platforms to account.

Do you think that the creation of a liability for platforms empowering citizens to take action for damage caused, like the law of torts, would be a way of holding platforms to account?

Mr. Jim Balsillie: One thing I can assure you is that when a board of directors or a CEO has to sign an attestation whereby they're personally liable, whether it's civil or criminal, I guarantee you, that sobers the mind and introduces a form of prudence and conservatism into their behaviour. If you introduce that tort or criminal construct and you get an attestation they have to sign, and if the citizens have the ability to be compensated for that, I assure you, that focuses the mind in the corporate boardrooms of tech companies and others, in my experience.

Mr. Ian Lucas: I raised the tort concept because we heard from the broadcasting regulator in the U.K. last week that she doesn't really consider that a regulator alone has sufficient flexibility or resources to deal with the scale of the challenge.

I wonder if we individualize the accountability through the development of a liability for the platforms whether that would be a way to empower citizens to take the action we need.

● (0915)

Mr. Jim Balsillie: I think you create liability, whether it's through class action or an individual or whether it's through regulators. I assure you, if it's corporate, that's one liability, but if it's personal and it ensnares....

The other thing is that it's one thing to be the CEO who is liable. If you're a board person who says, "My board fees aren't enough for me to be ensnared in this", that changes behaviour. If you introduce liability and shifts on that—how you specifically create somebody who can apply through the courts and all that is specific to each jurisdiction—it changes the decision approaches.

Ms. Jo Stevens (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): My question is to Roger McNamee.

What do you think Mark Zuckerberg is more frightened about—privacy regulation or antitrust action?

Mr. Roger McNamee: He is more afraid of privacy.

To Mr. Lucas, I would just say that the hardest part of this is setting the standard of what the harm is. These guys have hidden behind the fact that it's very hard to quantify many of these things.

The Chair: Thank you, Ms. Stevens.

We'll go to Mr. Erskine-Smith for five minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Because Mr. Picard has a copy of *The Age of Surveillance Capitalism* with sticky notes all over it and highlights, I'll pass my five minutes to him.

Mr. Michel Picard (Montarville, Lib.): My questions will start with Ms. Zuboff.

You talk about someone who is writing the music for us to dance to, so let's dance.

Your question at the beginning was whether the digital future could be our home. My reaction to that is that in fact the question should be whether the future home can be without digital.

Ms. Shoshana Zuboff: That's such an important distinction, because I don't think there is a single one of us in this room who is against the digital per se. This is not about being anti-technology. It's about technology being hijacked by a rogue economic logic that has turned it to its own purposes.

We talked about this a little last night, the idea that conflating the digital with surveillance capitalism is a dangerous category error. What we need is to be able to free the potential of the digital to get back to those values of democratization of knowledge and individual emancipation and empowerment that it was meant to serve and that it still can serve.

Mr. Michel Picard: That's where I thought we were going to go, because in your book you compared now to the industrial revolution, in which, although we were scared of the new technology, somehow this technology was addressed to people, for them to be the beneficiary of that progress. Now we are not the beneficiaries at all. It's, as you say, a *coup des gens*. It's not a *coup d'état*, so it's not a second step of this revolution. It's a situation in which people become the producers of the raw material and, as you wrote:

> ...Google's invention revealed new capabilities to infer and deduce the thoughts, feelings, intentions, and interests of individuals and groups with an automated architecture that operates as a one-way mirror irrespective of a person's awareness....

It's like the people connected to the machine in *The Matrix*.

Ms. Shoshana Zuboff: Yes, that metaphor is full of potential. It is true.

From the very beginning, the data scientists at Google who were inventing surveillance capitalism celebrated in their written patents and in their published research the fact that they could hunt and capture behavioural surplus without users ever being aware of these backstage operations. Surveillance was baked into the DNA of this economic logic and essential to its strange form of value creation, so it's with that kind of sobriety and gravitas that it is called "surveillance capitalism", because without the surveillance piece, it cannot exist.

Mr. Michel Picard: I'm in a world where I cannot live without digital, of course. I have two phones just for me. My fridge can talk to me now. We learned that a few weeks ago. It's everywhere.

Now I have to regulate all this. I have two possibilities. First, I will quote Mr. Schmidt at the Mobile World Congress and what he said when asked about government regulation, which was that the technology moves so fast that governments really shouldn't try to regulate it because it will change too fast, and any problem will be solved by technology. He said, "We'll move move much faster than any government."

Maybe I could have a comment from you, Professor, and also from Mr. Balsillie.

● (0920)

Ms. Shoshana Zuboff: I'm so glad you brought that up, because this is part of the relentless ideology of the surveillance capitalists. They have tried to put lawmakers on the run. They have tried to pit lawmakers against citizens. That "we serve the citizens" is exactly what is going on in Toronto right now: "Do you really want the government to take away these beautiful wooden buildings and these warm sidewalks that we're going to build for you?"

This is ideology. The fact is that they claim the right to freedom in the same way that Adam Smith and Friedrich Hayek argued that we need free markets and free market actors, because the marketplace is this ineffable mystery that no one can manage—*ergo*, freedom is necessary.

The surveillance capitalists claimed that freedom, but the market is no longer ineffable for them. They have total information. They know everything that's going in and out of their marketplaces. Surveillance capitalism knows too much to qualify for freedom. This is a rotten ideology at its core, and we must not be intimidated by it.

Mr. Michel Picard: I just have a few seconds—

The Chair: Thank you. We're out of time, Mr. Picard.

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

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair, and thanks to all of our witnesses this morning. It has been very enlightening.

While there seems to be general agreement that eventually harmonized legislation, regulation and policy development across the democracies may be a counter to surveillance capitalism, that doesn't seem likely any time soon.

Ms. Zuboff, last night you said that the "front line" in surveillance capitalism is Toronto, in Sidewalk Labs and the smart city project.

Mr. Balsillie, you've been quoted as saying that Sidewalk Labs is "a colonizing experiment in surveillance capitalism" and that Sidewalk Labs "continues to weaponize ambiguity".

For the two of you, perhaps Ms. Zuboff first and then Mr. Balsillie, has the City of Toronto been steamrollered—bamboozled—by Sidewalk Labs' razzle-dazzle, Mr. Doctoroff's vision, as it has gradually emerged?

Ms. Shoshana Zuboff: Of course I would cede to Mr. Balsillie, because he's been more on the ground there than I have, but in talking with the folks there, including Bianca Wylie, who is the citizen activist, and in reading everything that I have read, there's no question. I mean, this is how Sidewalk Labs operates.

They go into cities offering things that the municipality cannot afford and they do it for a quid pro quo—the suspension of law. They say, "We'll come into your city and provide all of these things, but we don't want to have to deal with policies and we don't want to have to deal with politics, so you're going to have to clean all that up if you want our money."

This is the direct bypassing of democracy in order to impose their vision, which ultimately is aimed at their own narrow commercial purposes.

Hon. Peter Kent: That was basically what Mr. Schmidt said some years ago: Give us a city to run and we'll run it.

Mr. Jim Balsillie: History will be very kind to those who are taking the leadership, like those around this table, and it will judge very harshly those who succumbed to their personal insecurities to be razzle-dazzled by these folks. Of course you can regulate. You have all the power to regulate. Of course you can. I think you can regulate very much in the near term. There are very clear surgical points that you can move to that will begin the shift, as everyone has mentioned. People like Ms. Ressa are calling for help.

Hon. Peter Kent: We've seen that Google has said, in response to new federal elections legislation on advertising, "We'll simply withdraw from accepting advertising."

Is it possible that big data could simply pull out of jurisdictions where regulations, in the absence of harmonized regulation across the democracies, are present?

● (0925)

Mr. Jim Balsillie: That's the best news possible, because as everyone has attested here, the purpose of surveillance capitalism is to undermine personal autonomy. Elections and democracy are centred on the sovereign self, exercising a sovereign will. Why in the world would you want to undermine the core bedrock of an election in a non-transparent fashion to the highest bidder at the very time your whole citizenry is on the line?

In fact, the revenue for this is immaterial to these companies. One of my recommendations is to just ban personalized online ads during elections. There are a lot of things you're not allowed to do for six or eight weeks. Just put that into the package. It's simple and straightforward.

Mr. Roger McNamee: There's one point that I think is being overlooked here, which is really important, and that is that if these companies disappeared tomorrow, the services they offer would not disappear from the marketplace. It would take literally moments. In a matter of weeks you could replicate Facebook, which would be the harder one. There are substitutes for everything that Google does that are done without surveillance capitalism. Do not in your mind allow any kind of connection between the services you like and the business model of surveillance capitalism. There is no inherent link there, none at all. This is something that has been created by these people because it's wildly more profitable.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up is Mr. Angus.

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

I'll say at the beginning that I represent a region that's bigger than the United Kingdom. I represent communities that have no roads, some of the poorest indigenous communities. Facebook and YouTube transformed the power of indigenous communities to speak to each other, to start to change the dynamic of how white society spoke about them. I understand it has incredible power for good.

I see more and more, though, in my region self-radicalized people, who are impossible to speak to. There are flat earthers—yes, there are; I've met them—anti-vaxxers, 9/11 truthers. I've seen the effect on our elections of the manipulation of anti-immigrant or anti-Muslim materials, but I had not yet seen the threat of death.

Ms. Ressa, you said yesterday that while in the west we face democratic threats, people are dying in Asia from the manipulation of these platforms. In an act of solidarity with our Parliament, with our legislators, are there statements that should be made publicly through our Parliament to give you support so that we can maintain a link with you as an important ally on the front line? I'd like to ask that as my first question.

Ms. Maria Ressa: Thank you.

Prime Minister Trudeau, when he visited Manila, was the only one of all the world leaders who were here at that point in time during APEC who mentioned human rights at all. Canada has been at the forefront of holding fast to the values of human rights and of press freedom.

Thank you in advance. I think the more we speak about this, the more the values are reiterated, especially since someone like President Trump truly likes President Duterte, and vice versa. It's very personal.

When you talk about where people are dying, you've seen this all over Asia. There is Myanmar. There is the drug war here in the Philippines. In India and Pakistan there are instances of this tool that is being used for empowerment, just as in your district, and being something that we do not want to go away, that we do not want to be shut down. Despite the great threats that I and my company face, Facebook and other social media platforms still give us the ability to organize and to create communities of action that had not been there before.

Mr. Charlie Angus: Thank you very much.

I've been very concerned about Sidewalk Labs. Looking at it as a real estate deal, this might be the most prime real estate in North America that was handed over to Google on what the Auditor General of Ontario said was the shortest RFP she's ever seen, of I think six weeks. It's 10 weeks for a local art project down there. Dan Doctoroff came and told us it was the longest RFP in history. The Auditor General raised concerns that there was no public involvement, that this was done behind the scenes. Dan Doctoroff told us that this was the most open process ever.

I'm very concerned about the privatization of public space. I come from mining country. We had company towns. We fought like hell to get rid of them.

I've heard from Mr. Balsillie and I've heard from Ms. Zuboff, so Mr. McNamee, what do you think the citizens of Toronto should do regarding giving Google that prime real estate in the downtown where so many people gather?

● (0930)

Mr. Roger McNamee: I wouldn't let them within 100 miles of Toronto. The fundamental issue here is one of self-governance and self-determination. I just don't believe that any business—not Google, not anybody—should be in the business of operating our public spaces and our civic infrastructure. There is a limit to what you can do with a public-private partnership, and that is way over the line.

There is an experiment going on in Barcelona, I believe, in a smart city project where the community and the citizens own the data. That will be a very interesting thing to watch.

The observation I would make is that I am still cautious about the gathering of the data in the first place. I believe that the underlying issues relative to surveillance create too many temptations for people. At the moment, it's way, way too difficult to monitor what they're doing with the data once it's collected. I believe that all of these things require, to use an old government phrase, dramatically more study before we move forward.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

Now we'll go to our delegations.

We'll go to the Parliament of Singapore for five minutes.

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

Thank you very much to all of you for your presentations this morning.

Mr. McNamee, you made the point that the business model of these platforms is really focused on algorithms that drive content to people who think they want to see this content. You also mentioned that fear, outrage, hate speech and conspiracy theories sell more. I assume by that you mean they sell more than truth does. Would that be right?

Mr. Roger McNamee: There was a study done at MIT in Cambridge, Massachusetts, that suggested that disinformation spreads 70% further and six times faster than fact. There are actually good human explanations for why hate speech and conspiracy theories move so rapidly. It's about triggering the flight or fight reflex.

Mr. Edwin Tong: Yes. When you throw in what Ms. Ressa said earlier about how disinformation is spread through the use of bots—I think she said that 26 fake accounts translated into three million different accounts that spread the information—I think we are facing a situation where disinformation, if not properly checked, goes exponentially viral. People get to see it all the time, and over time, unchecked, this leads to a serious erosion of trust and a serious undermining of institutions so that we can't trust elections, and fundamentally, democracy becomes marginalized and eventually demolished.

Would that be right, in your assessment?

Mr. Roger McNamee: I agree with that statement completely. To me, the challenge is in how you manage it. If you think about it, censorship and moderation were never designed to handle things at the scale that these Internet platforms operate at. In my view, the better strategy is to do the interdiction upstream, to ask the fundamental questions of what role platforms like this have in society and what business model is associated with them. To me, what you really want to do....

My partner, Renée DiResta, is a researcher in this area. She talks about the issue of freedom of speech versus freedom of reach, the latter being the amplification mechanism. On these platforms, what's really going on is the fact that the algorithms find what people engage with and amplify that more. Sadly, hate speech, disinformation and conspiracy theories are, as I said, the catnip that really gets the algorithms humming and gets people to react. In that context, eliminating that amplification is essential.

But how will you go about doing that, and how will you essentially verify that it's been done? To my mind, the simplest way to do that is to prevent the data from getting in there in the first place.

Mr. Edwin Tong: The point is that I think you must go upstream to deal with it, fundamentally, in terms of infrastructure. I think some witnesses also mentioned that we need to look at education, which I totally agree with, but when it does happen, and when you have the proliferation of false information, there must be a downstream or an end result kind of reach.

That's where I think your example of Sri Lanka is very pertinent, because it demonstrates that, left unchecked, the platforms would do nothing about the false information that goes around. What we do need is to have regulators and governments clothed with powers and levers to intervene swiftly and to disrupt the viral spread of online falsehoods very quickly.

Would you agree?

● (0935)

Mr. Roger McNamee: As a generalization, I would not be in favour of the level of government intervention that I have recommended here. I simply don't see alternatives at the moment.

In order to do what Shoshana is talking about and in order to do what Jim is talking about, you have to have some leverage, and the only leverage governments have today is their ability to shut these things down. Nothing else works quickly enough.

Mr. Edwin Tong: Yes, exactly. Speed is crucial in that situation. Look at what has happened in Sri Lanka, Myanmar and recently in Jakarta. That's what has happened.

Mr. Roger McNamee: Yes.

Mr. Edwin Tong: Thank you. My colleague will have some questions.

Ms. Sun Xueling (Senior Parliamentary Secretary, Ministry of Home Affairs and Ministry of National Development, Parliament of Singapore): I have some follow-up questions for Mr. McNamee. I'd like to make reference to the Christchurch shooting on March 15, 2019. After that, The New York Times published an article by Mr. Kevin Roose. I'd like to quote what he mentioned in his article. He said:

> ...we do know that the design of internet platforms can create and reinforce extremist beliefs. Their recommendation algorithms often steer users toward edgier content, a loop that results in more time spent on the app, and more advertising revenue for the company.

Those were his words. Would Mr. McNamee agree that the design of Internet platforms makes it easier for extremist views to thrive and gain a following?

Mr. Roger McNamee: Not only do I agree with that, I would like to make a really important point, which is that the design of the Internet itself is part of the problem. I'm of the generation—as Jim is as well—that was around when the Internet was originally conceived and designed. The notion in those days was that people could be trusted with anonymity, and that was a mistake, because bad actors use anonymity to do bad things. The Internet has essentially enabled disaffected people to find each other in a way in which they could never find each other in the real world and to organize in ways they could not in the real world.

When we're looking at Christchurch, we have to recognize the first step, which is that this was a symphonic work. This man went in and organized at least 1,000 co-conspirators prior to the act, using the anonymous functions of the Internet to gather them and prepare for this act. It was then, and only then, after all that groundwork had been laid, that the amplification processes of the system went to work. Keep in mind that those same people kept reposting the film. It is still up there today.

Ms. Sun Xueling: Yes, indeed.

The Chair: Thank you. We're past time, so if we have some time to get back around to finish your question, we will.

Next, we'll go to the Republic of Germany for five minutes.

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

I would like to start with Jim Balsillie. You mentioned in one of your six recommendations the question of taxation. As a member of our finance committee, I will say that this is, in many areas, an important aspect. Can you go a little deeper?

You mentioned especially the question of taxation of advertising. Do you see more areas there? Especially in the digital world, we know the problem of the shifting between countries and how difficult it is for countries to do a proper taxation.

Mr. Jim Balsillie: Sure. I'm talking about those who are buying the ads. Really, the core problem here is that when they're ad driven—you've heard extremely expert testimony on this—they'll do whatever it takes to get more eyeballs. The subscription-based model is a much safer place to be, because it's not attention driven.

One of the purposes of a tax is to manage externalities. If you don't like the externalities we're grappling with and that are illuminated here, then disadvantage those. Many of these platforms are moving more towards subscription-based models anyway, so just use tax as a vehicle to do that. The good benefit is that it gives you revenue. The second thing it could do is also begin to shift toward more domestic services. I think a tax has not been a lever that's been used, and it's right there for you.

Mr. Jens Zimmermann: Thank you. Maybe I'll make one comment on accountability.

From the experience we had in Germany with the introduction of our law, the so-called NetzDG, I would say that the aspect of accountability is one of the frequently mentioned aspects from which the networks have a lot of headaches, because at that point it's really getting personal, so I completely agree with what you said.

Professor Zuboff, I would like to ask you about the support of new forms of citizen action, which you mentioned. Being elected officials here, we know exactly how important it is to also convince the public, our voters. Also, from our experience in Germany, we know that many users have a lot of fear of something like what Roger McNamee mentioned—that we will shut it down. I don't know if we would exactly earn a lot of praise for doing that. We would have a lot of problems with our citizens.

How would you say we could encourage the users—the citizens—that some steps like these are needed? How can we avoid having that perceived as some sort of censorship by governments? We are always in that area where government interference can also be perceived as censorship.

● (0940)

Ms. Shoshana Zuboff: It's so critical to be conscious of that balance. Obviously, authoritarian governments would love Roger's recommendation—shut it down, because we don't like what they're saying. Obviously, that's not the intention here, so how do we make that distinction?

One thing I can say is that I really think we are in the midst of a sea change in this public reaction. I wonder if you're seeing this in Germany. I've been travelling all over the world, to many cities, over the last five months, continuously. With every group I talk to, I begin with one question: What are the concerns that brought you here?

In all different parts of the world and in every single group, no matter where I am, they say the same things. I ask them to shout out one word. It begins with “anxiety”, “manipulation”, “control”, “fear”, “resistance”, “democracy”, “freedom”, “rebellion”, “malaise”—the same constellation. What I've learned is that there is a sense, within our populations, that things are not right, that there is a power that is not aligned with our interests, that we don't understand it and that no one can control it.

That is beginning. With Cambridge Analytica, with Chris Wiley, our work is all making a difference. I think there is a ripeness there.

My advice would be to look to those areas where these new crystallizations are already emerging. Barcelona is one, which is based entirely on citizen solidarity. There are other cities as well that are getting on that bandwagon. There are groups of digital workers who are trying to devise digital communities and digital sovereignty.

It's about amplifying these things that are already coming up from the grassroots. The other side—and Maria was mentioning this as well—is education. We're still in a situation where every piece of peer research shows us, over and over again, that so many people simply do not understand these backstage operations. Why? Because billions of dollars have gone into designing them to keep us ignorant.

We have to break that, and we have to communicate and educate.

The Chair: Thank you very much.

Next up, we have the Republic of Chile.

Apparently the representative isn't here yet, so we'll go next to the representative from Estonia, for five minutes.

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

Thank you very much for those inspiring presentations to kick off the morning.

I will start with a question to Mr. McNamee. My reading and my understanding are that it is really difficult to force the toothpaste back into the tube once it is out. I do think that the use of artificial intelligence—algorithms—is here to stay. To be very fair, AI is not evil per se.

I would put my question this way: If you were sitting in my chair today, what would be the three steps you would recommend, or would take, if we leave shutting down the platforms aside for a second?

● (0945)

Mr. Roger McNamee: The issue that we're dealing with here is that in the United States, or in North America, roughly 70% of all the artificial intelligence professionals are working at Google, Facebook, Microsoft or Amazon. To a first approximation, they're all working on behavioural manipulation. There are at least a million great applications of artificial intelligence. Behavioural manipulation is not on them. I would argue that it's like creating time-release anthrax or cloning human babies. It's just a completely inappropriate and morally repugnant idea, yet that is what these people are doing.

To Mr. Zimmermann's point, I would simply observe that it is the threat of shutting them down and the willingness to do it for brief periods of time that creates the leverage to do what I really want to do, which is to eliminate the business model of behavioural manipulation and data surveillance. I don't think this is about putting the toothpaste back in the tube. This is about formulating toothpaste that doesn't poison people.

I believe this is directly analogous to what happened with the chemical industry in the fifties. The chemical industry used to pour its waste products—mercury, chromium and things like that—directly into fresh water. They left mine tailings on the sides of hills. Petrol stations would pour spent oil into sewers, and there were no consequences so the chemical industry grew like crazy and had incredibly high margins. It was the Internet platform industry of its era. Then one day society woke up and realized that those companies should be responsible for the externalities that they were creating. That is what I'm talking about here.

This is not about stopping progress. This is my world. This is what I do. I just think we should stop hurting people. We should stop killing people in Myanmar, in the Philippines, and we should stop destroying democracy everywhere else. We can do way better than that. It's all about the business model.

I don't want to pretend I have all the solutions. What we know is that the people in this room are part of the solution, and our job is to help you get there. Don't view anything I say as a fixed point. View this as something that we're going to work on together.

The three of us are happy to take bullets for all of you, because we recognize it's not easy to be a public servant with these issues out there. But do not forget you're not going to be asking your constituents to give up the stuff they love. The stuff they love existed before this business model. It will exist again after this business model.

Ms. Keit Pentus-Rosimannus: Coming from a country where basically all the life is all so digital, I very much agree that it doesn't mean stopping the progress.

I will continue now with Mr. Balsillie. You, several times, underlined the need to regulate the political micro-targeting, or the political parties' ads. I must bring the example from 2007 when Estonia was for the first time under a very massive and serious cyber-attack. The main target of this attack was not the government sector, but it was mainly the private sector. As I saw, a lot of damage can be done, targeting also anything but party politics.

Do you see that the regulations need to be different for political micro-targeting and all the other ads, or do you see that basically the rules are needed the same way in both sectors?

Mr. Jim Balsillie: I agree with Roger that it needs to be in both sectors, but if there's one that's uniquely pernicious it's the underpinnings of our democracy. I think there needs to be complete transparency of all activities between political parties and these platforms. I think political parties should be under privacy legislation. Believe it or not, in Canada our political parties are not governed by our privacy legislation. I think it requires a special kind of personalized ban during elections.

I do agree with Roger that the business model is fundamentally flawed. It's going to take a constellation of activities to get there, but I think the political place is the most sensitive and most targetable place to fix it right away.

Ms. Keit Pentus-Rosimannus: A lot of damage can be done by micro-targeting ads concerning the environmental damage, for example, or medicine, or several other sectors.

My last question would be—

● (0950)

The Chair: We're actually out of time. We're already at six minutes, so we'll move on. I do think we'll have some time to get back to another round. We see some of the delegations haven't arrived yet.

We'll go next to Mexico.

Hon. Antares Guadalupe Vázquez Alatorre (Senator, Senate of the United Mexican States): Thank you. I am going to speak in Spanish, if you'll allow me.

[*Delegate spoke in Spanish, interpreted as follows:*]

In Mexico, our present president recently participated three times in elections. Every single time he was censored in the traditional media to the point that, thanks to the social networks, we were able to communicate among citizens. This enabled democratization, so there was greater participation in Mexico in recent times.

However, we also have to face another question that has to do with the bots, as we call them—that is to say robots—so that we can diffuse trends in Twitter, Facebook, and so on that are trying now to undermine our regime. There are authors in Mexico that talk about the fourth-generation war that has to do with the diffusion in social networks.

Last weekend, we had a situation where one individual, who was part of the president's cabinet, left his post. On Twitter we started seeing that the president would name and appoint a corrupt person for the environment. They then started saying that the president was corrupt, because he wanted to appoint someone who was corrupt. That was never the idea. Yesterday, he appointed another person. Even though this was made clear, nothing happened.

How can we face this type of situation of democracy and anti-democracy that is favoured on social networks? Of course, it allows people to participate, but we also see the generation of these trends.

There's another topic that has to do with what Maria Ressa has suffered. This sexting issue for a woman is something that has to do with the international sphere, because we've known of many cases where we go to all these national entities and there's nothing to do, because essentially there is no legislation. At the same time, this transcends borders. What we have to do is go to Google. Google becomes something of a tribunal, an international court. It's very difficult to get rid of these images. We've seen suicides. We've seen people that have done terrible things because of this. What can we do at an international level? How can we work together, men and women, for this to end once and for all?

Thank you.

Ms. Shoshana Zuboff: We're surfacing this theme over and over again. If you think about the history of science and engineering in the 20th century, the whole idea was that systems would be created to cure and to provide fail-safe for any problems. In medicine, for example, the idea was vaccines that could counter viruses. In engineering, it was backup systems, fail-safe systems, layers of systems that could counter crises when they occurred—safety.

It's extraordinary that the Internet has been loosed upon the world to launch viruses without vaccines and to create channels for the kinds of things you are describing—the robots and the disinformation—without any kind of fail-safe system. As we've been discussing, this goes back to a fundamental problem, which is that there is no such thing as content moderation. There are only behavioural surplus supply chains and the idea of protecting these flows of behavioural data. Everything the platforms do is down a very narrow line. The only action that emerges is if they're in danger of losing user engagement, abusing surplus flows, or on the other hand, if they're in danger of attracting legal scrutiny.

Other than that, there is no action that they are programmed to take, because it is fundamentally an existential threat to do anything that limits behavioural surplus flows, the data flows.

That's where we have the opportunity, and you have the opportunity, to create those interventions when there are.... I don't think it can be just a knee-jerk reaction to the problems that the president confronted at a certain moment. We have to think more systemically, and go back to the root causes. Otherwise, we are in danger of falling into the problems that Mr. Zimmermann was referring to, which are that our governments are seen as self-serving.

We have to devise these fundamental mechanisms that we insist upon: that there can be no virus without vaccine, and that there have to be routine ways for lies to be stopped. That is an existential threat to surveillance capitalism. Therefore, we go back to the foundations here of addressing the economic logic. That's going to cover the sexual assaults in the social network, as well as the political assaults. All of these are captured by the same economic contradiction.

● (0955)

The Chair: Thank you very much.

Next up, we'll go to Morocco, for five minutes.

Mr. Mohammed Ouzzine (Deputy Speaker, Committee of Education and Culture and Communication, House of Representatives of the Kingdom of Morocco): Thank you, Mr. Chair.

Let me first of all thank you, organizers and co-organizers, for making this meeting the event that it is today.

I've been attentive in following the precious and valuable interventions, which were all trying to convey ideas and thoughts regarding protection of personal data on the one hand and the correlation between this protection and democracy on the other, which is ultimately the core of the topic.

Needless to remind you, violating private lives is shaking, if not jeopardizing, our democratic choices. That is, the retention of personal data by certain actors, be they state actors or trade actors, renders our democracies vulnerable and subject to manipulation. Today, whether we like it or not, we all become nomophobic, to the extent that this reminds me of Mary Shelley's *Frankenstein*. We become victims of our machines.

I have heard Shoshana speak of the failure of legislators to devise laws and enforce frameworks. Galileo once said, “You cannot teach a man anything; you can only help him discover it within himself.” I guess this is what we need to grasp today, more than ever before, beyond the restrictions, beyond the laws and beyond the regulations.

Don't you think—my question is directed to Shoshana—that it's an ethical question? Nobody can legislate on ethics, but what is frightening today is that the more it stays, the more it's going to be hard to handle.

How would you react to that?

Ms. Shoshana Zuboff: This is such a wonderful question. I realize I didn't have time this morning to share this with you, but it's in my written statement.

There's a fascinating story here about a U.S. Senate subcommittee that was convened in 1971, chaired by a famous senator, Sam Ervin, who was one of the Watergate senators who defended democracy in that crisis. It was a bipartisan committee, with everyone from arch-conservative Strom Thurmond to Ted Kennedy. It was convened around the subject of behavioural modification, because behavioural modification had been imported from the Cold War into civil society and was now being used in schools, hospitals, prisons and all kinds of institutions of captive populations. Sam Ervin wrote the conclusion for this committee. He said that behavioural modification fundamentally undermines individual sovereignty and robs people of autonomy, and without individual sovereignty and without autonomy there can be no freedom, and without freedom there can be no democracy.

The outcome of four years of deliberation on that subcommittee was to eliminate all federal funding for behavioural modification programs. That was in the 1970s. I think of the 1970s as five minutes ago. Those were some of the best years of my life. It wasn't that long ago. They were talking about aiming this at these institutions, bounded organizations. Here we are in 2019 and we have global architectures of behavioural modification backed by trillions of dollars of capital. Where is the outrage? Where is the moral compass? Where is the response within us, as you say, that says, “This cannot stand.” This is inimical to everything that our societies are founded on.

I agree with you. Part of our challenge now is to get over the ideologies of the last four decades that have belittled government, that have belittled the state and that have denied regulation as an assault on freedom. The challenge is to understand, as I said before, that these companies know too much to qualify for freedom. We need to “only” democracy. Survey everything on the horizon. Only democracy means only you have the power and the capability and the tools to intervene on this process before it is too late.

I have just one tiny little comment about something that was said earlier. It won't be done in a year. I think you brought this up, Mr. Kent: the time frame. This kind of change, this kind of structural transformation, is not the work of a day or a month or a year, but it can be done in five years. Maybe in five years—certainly in the next decade—we have a horizon to shift the *Titanic*. We have the time and the capabilities to do that. What we need, as you've just said, is to get in touch again with our moral bearings. They are there and we should not be intimidated.

● (1000)

The Chair: Thank you, Ms. Zuboff.

Next up we'll go to Costa Rica.

Ms. Carolina Hidalgo Herrera (Member, Legislative Assembly of the Republic of Costa Rica): [*Delegate spoke in Spanish, interpreted as follows:*]

I'd like to share two things with you that we've been doing in Parliament in Costa Rica, and also the presidency of the republic, to take care of these effects.

Recently the president of the country spoke against a group of trolls whom she was able identify because they were disseminating fake news. As a result we have created mechanisms of double check, truth hashtag trends about fake news. We have also created a hashtag to check the information that is broadcast, #LetThemNotLieToYou. It is rather a movement of checking the information on civil society for those who want to have the truth.

This has, in a way, softened things, but we have the debate, indeed, whether the possibility of creating these rules implies limiting freedom of expression. Social movement has had a greater effect than the debate in Parliament. I wanted to share that since the president was the one speaking about it. This has been very important in disseminating information.

● (1005)

The Chair: Ms. Ressa, do you have any comments? We haven't heard from you in a little while.

Ms. Maria Ressa: Part of what we're still seeing here is the debate centring on the gatekeeping part.

I'll look at it in the context of journalism standards and ethics, which are the values for content moderation, as Shoshana said. Gatekeeping is behaviour modification. Journalists have always had the ability to do that, but the reason we didn't before was precisely because we were held accountable. There was still a self-regulating function.

I think to just do a very simple action.... What I'm worried about sometimes, even though we're under attack, is that this would be throwing the baby out with the bathwater. Transparency was mentioned by Shoshana: transparency, accountability and then consistency. I think we're seeing creative destruction right now, and I think jumping to turn it all upside down without starting with pulling one thread may throw the baby out with the bathwater.

The Chair: Thank you, Ms. Ressa.

We'll go to the last country that's going to ask a question, Saint Lucia. We will have time for Singapore and Estonia to ask one more question each.

Go ahead.

Mr. Andy Daniel (Speaker, House of Assembly of Saint Lucia): Thank you, Mr. Co-Chair.

I come from a country or region where it was once said—or it's still being said, I suppose—that when the first world sneezes we catch a cold. We never understood or we never knew.... We participated in Facebook on their platforms, but until the 2016 American election, we never knew what effect they were having on us. That's when we got to know about Cambridge Analytica and the other platforms' involvement in our own domestic elections.

We being untouched territory, so to speak, what advice would you have for us in our region as to how we protect ourselves moving forward? It almost seems like the first world has the plague. We do not want to catch it. How would you suggest we go about protecting ourselves?

Mr. Jim Balsillie: I'll begin. I'll bookend it.

I think you have a forum here where you're learning from each other, and it's too much to ask for each individual to learn by themselves. Plus, these companies are very sophisticated at playing you off one another, so I would encourage you to find a way to institutionalize your forum as something that others can join and preserve so that you can manifest best practices. I think that will protect you on one end.

One thing we haven't touched much on today is the very profound benefit we've had from whistle-blowers who have really opened our eyes on these things. We learn about that activity through whistle-blowers, both the private sector and the public sector. In the suite of things that you're going to do, make sure that whistle-blower protection for both government and the private sector is something you enshrine both individually and collectively.

Ms. Shoshana Zuboff: I really want to add to and underscore what Jim just said. There is an opportunity here for a collectivity, for this group to begin to identify some of the kinds of interventions, policy interventions and regulatory actions, that you want to experiment with. There may be different countries here that become the living laboratory for some of these experiments, but you're not out there doing it alone. You're doing it with your colleagues. Everyone is monitoring, everyone is learning and everyone is helping to fine-tune, and then everyone is involved in the migration of best practice across the conversations that are taking place in each nation.

I really want to encourage you to pursue the question but to do it in a way that helps build this institutional vision that Jim is describing because that is what is going to move our shared societies forward.

● (1010)

Mr. Roger McNamee: Mr. Daniel, I think you have an enormous problem trying to solve this by yourselves. I think that Google doesn't believe that it's competing against Facebook. Facebook doesn't believe it's competing against Google. I think Google thinks it competes against the Government of China where the technology companies report to the government, and I think Google views itself as in competition at that level and that countries are, at best, subsidiary to them. I think they're unbelievably clever at playing countries off against each other, and they're very clever at essentially delaying long enough so that it becomes impossible to act.

The business model is the issue. It is pervasive and, for a smaller-scale country, the degrees of freedom available to you are very limited. Again, I hate to keep coming back to the Sri Lanka example, but as far as I can tell.... I don't care what scale your country's at. I think this is just as true of the United States. I don't think the United States has any leverage over these guys at all, short of shutting them down or at least threatening to shut them down.

What we have to do is to develop some leverage, and that is really what the challenge is for this committee and for policy-makers around the world. You have to recognize that what you're dealing with here is something that's really big. It's really new, and they have absolutely no intention of co-operating. You have no leverage over them—none. Until somebody shows that they're serious about doing something about this, it's just going to keep going on.

The Chair: Thank you, Mr. McNamee.

We'll go next to Singapore and then Estonia.

You'll have one last question each.

Ms. Sun Xueling: Mr. McNamee, in your book you say that:

> Whether by design or by accident, platforms empower extreme views in a variety of ways. The ease with which like-minded extremists can find one another creates the illusion of legitimacy. Protected from real-world stigma, communication among extreme voices over internet platforms generally evolves to more dangerous language.

Do you agree that, by providing a place for extremist content to thrive and for like-minded people with extreme views to gather, the tech companies bear some responsibility for grave attacks such as the Christchurch shooting?

Mr. Roger McNamee: The answer is that I do believe that they bear responsibility. Again, to go back to the answer I gave you before, we also have to remember the things that are inherent in the architecture of the Internet. To me the question is this: Is there some way to put anonymity on trial and have a conversation about whether identity is something that's fundamental? If you're going to have a right to free speech, do you have to be honest about who you are?

I think this is a really difficult thing and it's way above my talent level to answer that question, but what I think the companies are guilty of is the amplification. It is their design that amplifies hate speech. It is not their design that allowed those people to congregate. It is true that in other contexts they do allow them to congregate, and in that particular one the congregation took place in things like 8chan and Reddit. This is a super-difficult problem and sometimes you're going to see that the getting together.... I mean, obviously what the Russians did in the United States in 2016 took place inside Facebook and inside Instagram.

Yes, they do have responsibilities but, again, I think these things are really hard to parse and I look forward to working with you going forward because I do not want to pretend like I've got a snap answer for that.

The Chair: Thank you.

I'll go to Estonia for the next question.

Ms. Keit Pentus-Rosimannus: Thank you.

Disinformation campaigns have really been part of Estonia's big neighbour's wonderful methodology for ages. Russia's hybrid warfare has already been there for a long time. I would say that everything that helps to destabilize or distract the societies will be used and has been used. This is why I said before that, even today, if we already had the regulations in place for political parties, for how they use the data, it would not solve all the problems. Yes, it would be necessary for sure, and Estonia has been one of the countries that has been a strong believer that the rules that apply off-line also have to apply online, but it's not enough if we say that it's only the problem of political parties because it is not. It's much wider.

My question would actually be about GDPR. Again, coming from Europe, we have had our own very intense debates. The GDPR has been in effect now already for some time, and since the beginning of GDPR we have actually received 95,000 data protection complaints through the national authorities, which shows a little bit the demand that is there.

I would like your comment. How do you see the GDPR regulations when it comes to the protection of personal data?

● (1015)

Mr. Jim Balsillie: If I may, I think GDPR is an excellent step forward. I think the control elements of personal data and the portability and the consent aspects, and I believe the shift to more algorithmic integrity, are great steps forward. I think that's really powerful.

I think all the folks around this committee should reflect on the fact that, I believe, under article 8 of the EU constitution they've drafted GDPR as a universal human right so I, as a Canadian, can demand all my data controlled from Canada under EU law or they're breaking European legislation. I think how you can play these various jurisdictional regimes and structures is a very powerful set of possibilities, and I think Europe is showing a model for the world. I think it's a journey.

I think Roger hit upon something extremely important, which is paying attention to the identity aspects. Traditionally, governments gave you credential identity called passports and driver's licences and I think that's been a gap in the Internet and its design—and Tim Berners-Lee would say that. Perhaps government should come back into that role of saying, we'll be looking after identity, and that's a form of vertical state investment that you could explore here and could address much of the problem at a very surgical level.

Mr. Roger McNamee: May I add something about GDPR?

I worry about the next step. You have to expand what it covers. You have to address not just the data that people put into these systems but the data that is systematically gathered about them through acquisition from third parties, through surveillance tools like Alexa and through web tracking. The fact that none of that is covered is a huge issue.

Then obviously you have to have a regulatory enforcement policy that puts teeth into it, because the fines are trivial and the processes take way too long and none of that's having any impact. You can see that fines of billions of euros have no impact on these companies. It needs to be tens of billions of euros and it needs to be every month. You have to get their attention. Right now, Facebook wants to move everything to the current version of GDPR because it prevents their competitors.... The cost is so much higher on their competitors, it's an enormous advantage to them and it doesn't touch any of the surveillance capital concepts that they're excited about.

The stupidity of Facebook and Google was that they didn't embrace it right off the shoot and actually implement it.

The Chair: Thank you.

That brings us to the conclusion of the questions. I'll just summarize some of the comments.

Ms. Zuboff, you mentioned the term “behavioural modification”. Ms. Ressa, you talked about “creative destruction”. Mr. Balsillie, you talked about undermining our personal autonomy.

Last night, because I had nothing better to do, I was watching CPAC. I was watching you, Mr. McNamee, and you referred to our audience and our users, and you used a particular name. As legislators our challenge is to relate to the millennial generation in terminology that we can all easily understand. You mentioned the term “voodoo dolls”. I would like you to finish off with an explanation of what that is and how you explained it last night, because I really couldn't think of a better way to explain what's happening to our generation.

● (1020)

Mr. Roger McNamee: When they gather all of this data, the purpose of it is to create a high resolution avatar of each and every human being. It doesn't matter whether you use their systems or not. They collect it on absolutely everybody. The concept of voodoo in the Caribbean was essentially this notion that you create a doll, an avatar, and that you can poke it with a pin and the person would experience that pain, so it becomes literally a representation of the human being.

My partner, Tristan Harris, came up with this notion of the voodoo doll to describe what's going on here, because what happens is that, before long, you get to this point where you can anticipate what people are going to be able to do. Because of the resolution of the voodoo doll and the context of all the other voodoo dolls you have, you can see what people who have common characteristics have done and it tells you what this person is going to do.

Shoshana makes the core point that, at the beginning, it's about trying to anticipate, but ultimately, in the final analysis, it is about actually manipulating behaviour, and the way you do this is by controlling the menu.

We as consumers think that Google is an honest broker, that Facebook is an honest broker and that the results of our queries are honest, but they're not. They are informed by the data voodoo doll, and as a consequence they are manipulating our behaviour because they manipulate the choices that are available to us.

Just as with a voodoo doll in the Caribbean, you are not aware of it. You're just aware that the outcome has happened without understanding what the source of it was. I think that is just wrong. As policy-makers and as somebody who spent 35 years in Silicon Valley, it's our job to come to the defence of our constituents.

The Chair: Thank you, Mr. McNamee.

I would like to thank you all for testifying and the offer Ms. Zuboff made to us to help us get there. We're going to be calling on you. This committee will end tomorrow at noon. Certainly though, the work will not. We look forward to having your opinions as a feedback loop and also to ask you questions on a regular basis to get the answers we need.

We're going to have the platforms appear at 10:30. That's in 10 minutes.

Thank you again for appearing before us today.

The meeting is adjourned.