HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 151 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Monday, May 27, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Monday, May 27, 2019

● (1900)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): We'll call to order our meeting of the Standing Committee on Access to Information, Privacy and Ethics, and to a larger extent, our international grand committee.

We'd like to welcome especially the visitors from around the globe tonight.

You will notice some empty seats beside you. We've heard of some unexpected flight delays for some of the delegations. They will definitely be here. Some are arriving as we speak. Some are arriving in about an hour from now. Again, my apologies for their not being here as planned.

I'd like to go through, first of all, the countries that are going to be represented tonight, tomorrow and Wednesday. Then we'll go around and have some brief introductions, and get right into the presentations.

We're still expecting some of our witnesses to come, as well.

We'll start off with the countries that are represented, confirmed just today—Canada, of course, the United Kingdom, Singapore, Ireland, Germany, Chile, Estonia, Mexico, Morocco, Ecuador, St. Lucia, and Costa Rica.

I will say that we have lost a few due to something called elections around the globe that we can't really have control over. Those have gotten in the way of some of the other countries being able to get here.

I see some of our witnesses. Mr. Balsillie and Mr. McNamee, please take your seats at the front. We're just getting started. Welcome.

I want to go around the table quickly and have the delegates say their name and introduce the country they're from.

Let's start off with our member from Estonia.

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

I am Keit Pentus-Rosimannus, representing the Estonian Parliament today.

Ms. Sun Xueling (Senior Parliamentary Secretary, Ministry of Home Affairs and Ministry of National Development, Parliament of Singapore): Hi, everyone.

I am Sun Xueling. I'm the senior parliamentary secretary, Ministry of Home Affairs and Ministry of National Development, from Singapore.

Thank you.

Mr. Edwin Tong (Senior Minister of State, Ministry of Law and Ministry of Health, Parliament of Singapore): Good evening, everyone.

I'm a member of Parliament from Singapore and also Senior Minister of State in the Ministry of Health and Ministry of Law in Singapore.

Thank you.

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

My name is Jens Zimmermann. I'm a member of the German Bundestag, and I'm the spokesperson on digitalization for the Social Democrats.

Mr. Charlie Angus (Timmins—James Bay, NDP): I am Charlie Angus, vice-chair of this committee and a member of the New Democratic Party. I represent the constituency of Timmins—James Bay, which isn't a country, but it is larger than France.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): I'm Jacques Gourde, Conservative member for Lévis—Lotbinière.

[*English*]

Hon. Peter Kent (Thornhill, CPC): I am Peter Kent, the member of Parliament for Thornhill on the northern city limits of Toronto. I am the critic for the official opposition, the Conservative Party, on the ethics committee, which is responsible for ethics, lobbying, information and privacy.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): I'm Nate Erskine-Smith. I'm a Liberal member, representing a Toronto area riding called Beaches—East York. I'm the Liberal vice-chair of this committee.

Mr. Raj Saini (Kitchener Centre, Lib.): My name is Raj Saini. I'm the member of Parliament for Kitchener Centre. I'm a Liberal member. I also sit on the foreign affairs and international development committee.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): I am Anita Vandenbeld. I'm the Liberal member of Parliament for Ottawa West—Nepean, which is about 15 minutes west of here. I'm also on the foreign affairs committee and chair of the Subcommittee on International Human Rights.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): My name is David Graham. I represent the riding of Laurentides—Labelle, which is a much smaller riding than Charlie's, but it is much bigger than Singapore. I'm on four other committees. In terms of this one, I'm not a regular member but I am a regular member, if you can call it that.

Thank you for this.

● (1905)

The Chair: Thank you.

I'll finish.

My name is Bob Zimmer, member of Parliament for Prince George—Peace River—Northern Rockies, the beautiful northern British Columbia riding with the Rockies running right through it. I also chair the access to information, privacy and ethics committee that we sit before tonight.

Also, I'll give Mr. Kint some credit today. I gave you some credit earlier. This whole idea of the international grand committee came out of a Washington summit meeting in a pub with me, Mr. Erskine-Smith, Ian Lucas and Damian Collins. That's how it really started. We wanted to do something better—we thought better together as a coalition of countries to work out some solutions to these problems. So I'll give you some credit for probably buying one of the beers that one night. I appreciate that.

Mr. Angus has a comment, and then we'll get into the presentations.

Mr. Charlie Angus: I'm sorry to interrupt, Mr. Chair, but I just wanted to confirm that our committee, through all-party consensus, issued a subpoena to Mr. Zuckerberg and Ms. Sandberg. I do believe that's unprecedented. I am reading reports that Facebook is speaking to media, saying they're not showing up to our committee. I am not aware whether they have officially responded to the subpoena.

Can you inform this committee whether they have bothered to respond to us on this issue?

The Chair: Yes, I've seen similar.... The story, I believe, was on CNN this afternoon. I have not received that, as chair of the committee. Whether they will show up or won't show up.... We've asked the clerk, as well. We haven't received any communication to say they're not going to be appearing tomorrow morning.

My expectation is that we'll have some spaces for them to come and sit and give testimony. Whether or not they choose to fill those is up to them.

Again, it's my hope and expectation that they will follow through with our subpoena and show up tomorrow. That's just my comment back that officially, nothing as chair, nothing as clerk of the committee.

Mr. Charlie Angus: Thank you very much.

The Chair: We'll get right into it tonight. It's a bit more of an informal presentation from our guests tonight, so we won't be asking questions. This is just setting the stage for the next couple of days. It's warming up the conversation on why we're here and why we need to be concerned about big data, privacy and disinformation, etc.

We'll start off with Mr. Kint.

We'll give you the floor.

First, I'll read the list so that you'll know when you're the next to speak, and maybe I'll say who you represent, although you're all here as individuals.

As I said, we're starting with Jason Kint.

Jim Balsillie, chair, Centre for International Governance Innovation.

Roger McNamee, author of *Zucked*.

Roger, I know your resumé goes a lot longer than that, but we'll keep it short.

Taylor Owen, associate professor, McGill University.

Ben Scott.

Heidi Tworek, assistant professor, University of British Columbia.

Shoshana Zuboff.

Shoshana, I really appreciated your book. It's very informative.

Last but not least is Maria Ressa. She is with us via teleconference.

We're glad you could join us tonight, Maria. I know that you've been in some trying circumstances of late. It would have been nice to have you here, but I understand that that's out of your control.

We'll start off with Jason, and next will be Jim.

Go ahead, Jason.

Mr. Jason Kint (Chief Executive Officer, Digital Content Next): Thank you for the opportunity to appear before the international grand committee. I am the CEO of the U.S.-based trade association Digital Content Next, and I appreciate the opportunity to speak on behalf of high-quality digital publishers.

We represent about 80 publishers globally. Many of them have offices in your home countries. They include the New York Times, the Wall Street Journal, the Financial Times, the BBC, the Guardian, Axel Springer. There are nearly 80 members. To be clear, our members do not include any social media, search engine or ad tech companies. That may be part of why I'm here.

DCN has prioritized shining a light on issues that erode trust in the digital marketplace, including a troubling data ecosystem that has developed with very few legitimate constraints on the collection and use of data about consumers. As a result, personal data is now valued more highly than context, consumer expectations, copyright and even facts themselves.

As policy-makers around the world scrutinize these practices, we urge you, along with industry stakeholders, to take action. We believe it is vital that policy-makers begin to connect the dots between the three topics of your inquiry: data privacy, platform dominance and societal impact.

Today, personal data is frequently collected by unknown third parties without consumer knowledge or control. That data is then used to target consumers across the web as cheaply as possible. This dynamic creates incentives for bad actors, particularly on unmanaged platforms like social media which rely on user-generated content mostly with no liability, where the site owners are paid on the click whether it is from an actual person or a bot, on trusted information or on disinformation.

We are optimistic about regulations like the GDPR in the EU which, properly enforced—that's important, properly enforced—contain narrow purpose limitations to ensure companies do not use data for secondary uses. We recommend exploring whether large tech platforms that are able to collect data across millions of websites, devices and apps should even be allowed to use this data for secondary purposes.

As an example of critically important action, we applaud the decision of the German cartel office to limit Facebook's ability to collect and use data across its apps and across the web. It's a very important decision.

The opaque data-driven ecosystem has strongly benefited intermediaries, primarily Google, and harmed publishers and advertisers. These intermediaries have unique leverage as gate-keepers and miners of our personal data. As a result, issues have surfaced including bot fraud, malware, ad blockers, clickbait, privacy violations and now disinformation, all over the past decade. However, importantly these are all symptoms. Make no mistake, the root cause is unbridled data collection at the most personal level imagined.

It is important to understand the power of these two companies. Four years ago, DCN did the original financial analysis labelling Google and Facebook the duopoly of digital advertising. The numbers are startling. In a $150-billion-plus digital ad market across North America and the E.U., 85% to 90% of the incremental growth is going to just these two companies. As we dug deeper, we connected the revenue concentration to the ability of these two companies to collect data in a way that no one else can. This means both companies know much of your browsing history and your location history. Data is the source of their power. The emergence of this duopoly has created a misalignment between those who create the content and the those who profit from it.

Finally, these data practices coupled with the dominance, without accountability, of these two companies is indeed impacting society. The scandal involving Facebook and Cambridge Analytica under-scores the current dysfunctional dynamic. Under the guise of research, GSR collected data on tens of millions of Facebook users. As we now know, Facebook did next to nothing to ensure that GSR kept a close hold on our data. This data was ultimately sold to Cambridge Analytica and it was used for a completely different purpose: to target political ads and messages, including the 2016 U. S. election.

With the power Facebook has over our information ecosystem, our lives and democratic systems, it is vital to know whether we can trust the company. Many of its practices prior to reports of the Cambridge Analytica scandal clearly warrant significant distrust.

● (1910)

Although there has been a well-documented and exhausting trail of apologies, it's important to note that there has been little or no change in the leadership or governance of Facebook, Inc. In fact, the company has repeatedly refused to have its CEO offer evidence to pressing international governments wanting to ask smart questions, leaving lawmakers with many unanswered questions.

Equally troubling, other than verbal promises from Facebook, it's not clear what will prevent this from happening again. We believe there should be a deeper probe, as there is still much to learn about what happened and how much Facebook knew about the scandal before it became public. Facebook should be required to have an independent audit of its user account practices and its decisions to preserve or purge real and fake accounts over the past decade. We urge you to make this request.

To wrap up, it is critical to shed light on these issues to understand what steps must be taken to improve data protection, including providing consumers with greater transparency and choice over their personal data when using practices that go outside of the normal expectations of consumers. Policy-makers globally must hold digital platforms accountable for helping to build a healthy marketplace, restoring consumer trust and restoring competition.

Thank you for your time. I appreciate the opportunity to discuss these issues with you today.

The Chair: Thank you, Mr. Kint.

You've kept very well under your seven-minute time. I'd like to remind everybody that seven minutes is the time allotted, so that was a good job.

Next up is Mr. Balsillie.

Mr. Jim Balsillie (Chair, Centre for International Governance Innovation, As an Individual): Thank you very much, Mr. Chair. I will take less than that because I will be giving formal comments to the committee tomorrow.

Mr. Chairman and committee members, it's my honour and privilege to testify today to such distinguished public leaders. Data governance is the most important public policy issue of our time. It is crosscutting with economic, social and security dimensions. It requires both national policy frameworks and international coordination.

In my testimony tomorrow, I will give more description, and then I will end with six specific recommendations. I will spend a couple of minutes today speaking to one of the recommendations that I would like to bring forward to the group, which is that you create a new institution for like-minded nations to address digital co-operation and stability.

The data-driven economy's effects cannot be contained within national borders. New approaches to international coordination and enforcement are critical as policy-makers develop new frameworks to preserve competitive markets and democratic systems that evolved over centuries under profoundly different technological conditions. We have arrived at a new Bretton Woods moment. We need new or reformed rules of the road for digitally mediated global commerce, a world trade organization 2.0.

In the aftermath of the 2008 financial crisis, the Financial Stability Board was created to foster global financial co-operation and stability. A similar global institution, say, a digital stability board, is needed to deal with the challenges posed by digital transformation. The nine countries on this committee plus the five other countries attending, totalling 14, could constitute the founding members of such a historic plurilateral body that would undoubtedly grow over time.

Thank you.

● (1915)

The Chair: Thank you, Mr. Balsillie.

Next up we have Roger McNamee. Taylor Owen is on deck.

Go ahead, Mr. McNamee.

Mr. Roger McNamee (Author of Zucked, As an Individual): I want to thank you for the opportunity to be here.

I come here as someone who has spent an entire professional lifetime involved in Silicon Valley building the best and brightest companies. The core thing I want you to understand is that the culture of Silicon Valley has come completely off the rails and that the technology industry today is committed to monopoly. It is committed to, as Professor Zuboff will describe, a form of capitalism that would be foreign to any of us who have grown up in the last 50 years.

In my mind, the industry has demonstrated that it is not capable of governing itself and that, left to its own devices, it will, as a matter of course, create harms that cannot easily be remedied. As a consequence, I believe it is imperative that this committee and nations around the world engage in a new thought process relative to the ways that we're going to control companies in Silicon Valley, especially to look at their business models.

The core issue that I would point to here, relative to business models, is that, by nature, they invade privacy, and that, by nature, they undermine democracy. There is no way to stop that without ending the business practices as they exist. I believe the only example we have seen of a remedy that has a chance of success is the one implemented by Sri Lanka recently when it chose to shut down the platforms in response to a terrorist act. I believe that is the only way governments are going to gain enough leverage in order to have reasonable conversations.

My remarks tomorrow will go into that in more depth.

I want to thank you for this opportunity. I want you to understand that I will be available to any of you at any time to give you the benefit of my 35 years inside Silicon Valley so you understand what it is we're up against.

Thank you very much.

The Chair: Thank you very much, Mr. McNamee.

Next up, we have Taylor Owen, and on deck is Ben Scott.

Go ahead, please.

Professor Taylor Owen (Associate Professor, McGill University, As an Individual): Thank you, co-chairs Zimmer and Collins, and committee members, for having me. I have to say it's a real honour to be here with you and amongst these other panellists.

I'm particularly heartened, though, because even three years ago, I think a meeting like this would have seemed unnecessary to many in the public, the media, the technology sector and by governments themselves. However, now I would suggest that we're in an entirely different policy moment. I want to make five observations about this policy space that we're in right now.

The first point I want to make is that it's pretty clear that self-regulation and even many of the forms of co-regulation that are being discussed have proven and will continue to prove to be insufficient for this problem. The financial incentives are simply powerfully aligned against meaningful reform. These are publicly traded, largely unregulated companies, which shareholders and directors expect growth by maximizing a revenue model that is itself part of the problem. This growth may or may not be aligned with the public interest.

The second point I want to make is that this problem is not one of bad actors but one of structure. Disinformation, hate speech, election interference, privacy breaches, mental health issues and anti-competitive behaviour must be treated as symptoms of the problem, not its cause. Public policy should therefore focus on the design and the incentives embedded in the design of the platforms themselves.

It is the design of the attention economy which incentivizes virality and engagement over reliable information. It is the design of the financial model of surveillance capitalism, which we'll hear much more about, which incentivizes data accumulation and its use to influence our behaviour. It is the design of group messaging which allows for harmful speech and even the incitement of violence to spread without scrutiny. It is the design for global scale that is incentivized in perfect automation solutions to content filtering, moderation and fact-checking. It is the design of our unregulated digital economy that has allowed our public sphere to become monopolized.

If democratic governments determine that this structure and this design is leading to negative social and economic outcomes, as I would argue it is, then it is their responsibility to govern.

The third point I would make is that governments that are taking this problem seriously, many of which are included here, are all converging I think on a markedly similar platform governance agenda. This agenda recognizes that there are no silver bullets to this broad set of problems we're talking about. Instead, policies must be domestically implemented and internationally coordinated across three categories: content policies which seek to address a wide range of both supply and demand issues about the nature, amplification and legality of content in our digital public sphere; data policies which ensure that public data is used for the public good and that citizens have far greater rights over the use, mobility and monetization of their data; and competition policies which promote free and competitive markets in the digital economy.

That's the platform governance agenda.

The fourth point I want to make is that the propensity when discussing this agenda to over-complicate solutions serves the interests of the status quo. I think there are many sensible policies that could and should be implemented immediately. The online ad micro-targeting market could be made radically more transparent, and in many cases suspended entirely. Data privacy regimes could be updated to provide far greater rights to individuals, and greater oversight and regulatory power to punish abuses. Tax policy could be modernized to better reflect the consumption of digital goods and to crack down on tax base erosion and profit-sharing. Modernized competition policy could be used to restrict and roll back acquisitions and to separate platform ownership from application and product development. Civic media can be supported as a public good, and large-scale and long-term civic literacy and critical thinking efforts can be funded at scale by national governments, not by private organizations.

That few of these have been implemented is a problem of political will, not of policy or technical complexity.

Finally, though, and the fifth point I want to make is that there are policy questions for which there are neither easy solutions, meaningful consensus nor appropriate existing international institutions, and where there may be irreconcilable tensions between the design of the platforms and the objectives of public policy.

The first is on how we regulate harmful speech in a digital public sphere. At the moment, we've largely outsourced the application of national laws as well as the interpretation of difficult trade-offs between free speech and personal and public harms to the platforms themselves: companies that seek solutions, rightly in their perspective, that can be implemented at scale globally. In this case, I would argue that what is possible technically and financially for the companies might be insufficient for the goals of the public good, or the public policy goals.

● (1920)

The second issue is liable for content online. We've clearly moved beyond the notion of platform neutrality and absolute safe harbour, but what legal mechanisms are best suited to holding platforms, their design and those who run them accountable?

Finally, as artificial intelligence increasingly shapes the character and economy of our digital public sphere, how are we going to bring these opaque systems into our laws, norms and regulations?

In my view, these difficult conversations, as opposed to what I think are the easier policies that can be implemented, should not be outsourced to the private sector. They need to be led by democratically accountable governments and their citizens, but this is going to require political will and policy leadership, precisely what I think this committee represents.

Thank you very much.

● (1925)

The Chair: Thank you, Mr. Owen.

We'll go next to Mr. Scott.

Dr. Ben Scott (As an Individual): Thank you very much, Mr. Chairman. It's a privilege and an honour to be here in front of this assembled international committee.

I appear before you this evening as an unlikely witness. I say that because I've spent pretty much my entire career promoting the virtues of the open Internet. I came of age during the Internet revolution of the late 1990s. I worked on the first truly digital political campaign for President Barack Obama in 2008. I was one of Hillary Clinton's digital diplomats in the heyday of Internet freedom during the Arab Spring. It was a moment in time when it seemed like smart phones and social media were the genuine catalysts of social and political movements to democratize the world. It was an inspiring moment. These technologies did help those things happen.

I'm an idealist at heart. I wanted to be in the middle of that revolution, but I sit before you today as a troubled idealist. I went back and worked for my old boss in 2016 on her presidential campaign. I ran the technology policy advisory committee. I had a ringside seat to what happened in America between 2015 and 2017. What I saw was that the open Internet that was meant to expand freedom instead turned into a powerful technology of social manipulation and political distortion. You all know the story. What was once the great hope for the revitalization of democracy is now considered by many to be among its greatest threats. My friends, that is a bitter irony—bitter—but it doesn't need to be that way.

The promise of information networks to distribute power to the people is a promise that we can reclaim, but we need to see at what point the astonishing control over wealth and power in this industry began to develop and steer things off course. The roots of this are deep, and we can track it back for decades, but I pinpoint a moment in time between 2014 and 2017 when machine learning technologies were applied to social media platforms, so-called artificial intelligence.

These technologies were not core to the Facebook and Google business models in 2011 and 2012 during the heyday of the Arab Spring. They arrived on the scene sometime later. If you want to know exactly when they arrived on the scene, look at the profit and revenue charts of Google and Facebook. I've written down the numbers for Facebook just to give you the case in point. In 2011, Facebook for the first time made $1 billion in profit on $4 billion in revenue. In 2017, just six years later, after the advent of these new technologies, they made $16 billion in profit on $40 billion in revenue. That's a more than 10x increase in six years.

How did that happen? It happened because they figured out a business model for superprofits. Step one: Track everything that billions of people do online and put it in a database. Step two: Sort that data and group people into target audiences and then sell access to their attention, engineering your entire information marketplace to optimize not for the quality of information or the civility of the dialogue in our society, but optimize just for addictiveness and time spent on the platform. Because the more time people spend on the platform, the more ads they see, and the more money the superprofits make.

It's a beautiful business model, and it works. It works with 10x profit in six years. Very few companies can claim anything like that kind of growth.

Also, it's not just the ads that get targeted. Everything gets targeted. The entire communications environment in which we live is now tailored by machine intelligence to hold our attention. This is not a recipe for truth and justice. What feels true performs better than what is true. Conspiracy and hate have become the organizing themes of social media, and that is a space that is easily exploited by propagandists peddling bigotry, social division and hatred to the disillusioned.

This is the connection between the data markets that we've heard talked about at this table and the abhorrent content you see online, whether we're talking about everyday hate speech or about something truly awful like the shootings in New Zealand. It is the algorithms that lead us into the temptation of our biases. This is what we have to address. We cannot rely on the industry to fix this problem.

● (1930)

The core problem lies at the heart of the business model, what Professor Zuboff calls “surveillance capitalism”, and these companies are kings of the market. Public traded companies—

The Chair: Just a second. The translation just went from English to Spanish, I believe. We'll just let the translators know.

I'm good at English, but not at Spanish.

Dr. Ben Scott: That's that machine intelligence coming in to steer you away from my testimony.

The Chair: Translation, are we good to go? Okay.

Go ahead, Mr. Scott. Sorry.

Dr. Ben Scott: I've spent the last two and a half years studying this problem, pretty much from the day I woke up after the U.S. presidential election in November 2016, and I'm convinced of the thesis that I've just laid out to you. However, I want to be clear: Technology doesn't cause this problem. It accelerates it. It shapes it. It shapes its growth and its direction. It determines in what ways social development and history flow. Technology is an amplifier of the intentions of those who use it. These consequences are, in my view, not inevitable. There's no technological determinism here. We can fix this.

Just as we made policy decisions to expand access to affordable Internet and to make net neutrality the law of so many lands—we did that to support the democratizing potential of the technology—we can now make policies to limit the exploitation of these tools by malignant actors and by companies that place profits over the public interest. We have to view our technology problem through the lens of the social problems that we're experiencing.

This is why the problem of political fragmentation, hate speech or tribalism in digital media, depending on how you want to describe it, looks different in each of your countries. It looks different in each of your countries because it feeds on the social unrest, the cultural conflict and the illiberalism that is native to each society. There are common features that stretch across the board, but each country is going to see this in a slightly different way.

To be fair, our democracies are failing a lot of people. People are upset for good reason, but that upset is not manifesting as reform anymore. It's manifesting as a kind of festering anger. That radicalism comes from the way technology is shifting our information environments and shaping how we understand the world. We rarely see the world through the eyes of others. We are divided into tribes, and we are shown a version of the world day in and day out, month after month, that deepens our prejudices and widens the gaps between our communities. That's how we have to understand this problem.

To treat this, this sickness, this disease, we have to see it holistically. We have to see how social media companies are part of a system. They don't stand alone as the supervillains, as much as we might like to brand them that way, although they carry a great deal of responsibility. Look and see how the entire media market has bent itself to the performance metrics of Google and Facebook. See how television, radio and print have tortured their content production and distribution strategies to get likes and shares and to appear higher in the Google News search results. It's extraordinary. It reinforces itself, the traditional media and the new media.

Yes, I completely agree with Professor Owen that we need a public policy agenda and that it has to be comprehensive. We need to put red lines around illegal content. We need to limit data collection and exploitation. We need to modernize competition policy to reduce the power of monopolies. We also need to pull back the curtain on this puppet show and show people how to help themselves and how to stop being exploited.

I think there's a public education component to this that political leaders have a responsibility to carry. We need to invest in education, and we need to make commitments to public service journalism so that we can provide alternatives for people, alternatives to the mindless stream of clickbait to which we have become accustomed, the temptations into which we are led as passive consumers of social media.

I know this sounds like a lot, but I invite you to join me in recommitting yourself to idealism. It isn't too much to ask because it's what democracy requires.

Thank you very much.

The Chair: Thank you, Mr. Scott.

Next up is Heidi Tworek, and on deck is Ms. Zuboff.

● (1935)

Dr. Heidi Tworek (Assistant Professor, University of British Columbia, As an Individual): Thank you so much, Mr. Chair.

Thank you to the distinguished members of the international grand committee for the kind invitation to speak before you today. It's really an honour to support international co-operation in this form.

In my work, I wear two hats. I'm a historian and I analyze policy. I know wearing two hats is a bit of a strange fashion choice, but I think it can help to lead us to much more robust solutions that can stand the test of time.

In my policy work, I have written about hate speech and disinformation in Canada, the United States and in Europe. I'm a member of the steering committee of the transatlantic high level working group on content moderation online and freedom of expression.

Wearing my history hat, I've been working for nearly a decade on the history of media. I just finished this book, which is called *News From Germany: The Competition to Control World Communications, 1900-1945*. Among other things in this book, I detail how it is that Germany's vibrant, interwar media democracy descended into an authoritarian Nazi regime that could spread anti-Semitic, racist and homophobic propaganda around the world.

While I was writing this book, the present caught up with history in all sorts of, frankly, disturbing ways. The far right around the world revived Nazi terminology using *lügenpresse* and *systempresse* —the lying press and the system press—to decry the media. Marginalized groups were targeted online and they were blamed for societal ills that they did not cause. News was falsified for political and economic purposes. Like with radio in the first half of the 20th century, a technology designed with utopian aims became a tool for dictators and demagogues.

As our other witnesses have described, some aspects of the Internet are unprecedented, such as the micro-targeting, the scale, the machine learning and the granular level of surveillance, but some of the underlying patterns look surprisingly familiar to the historians among us.

I'm going to offer five brief lessons from this history that I think can guide our policy discussions in the future and enable us to build robust solutions that can make our democracies stronger rather than weaker.

The first lesson is that disinformation is also an international relations problem. Information warfare has been a feature, not a bug, of the international system for at least a century. The question is not if information warfare exists, but why and when states engage in it.

What we see is that it's often when a state feels encircled, weak or aspires to become a greater power than it already is. This is as true for Germany a hundred years ago as it is for Russia today. If many of the causes of disinformation are geopolitical, we need to remember that many of the solutions will be geopolitical and diplomatic as well.

Second, we need to pay attention to the physical infrastructure of what is happening. Information warfare and disinformation are also enabled by physical infrastructure, whether it's the submarine cables a century ago or fibre optic cables today. One of Britain's first acts of war in World War I was to cut the cables that connected Germany to the rest of the world, pushing Germany to invest in a new communications technology, which was radio. By the time the Nazis came to power, one American radio executive would call it the most potent political agency the world had ever known.

We often think of the Internet as wireless, but that's fundamentally untrue; 95% to 99% of international data flows through undersea fibre optic cables. Google partly owns 8.5% of those submarine cables. Content providers also own physical infrastructure. Sometimes those cables get disrupted because they get bitten through by sharks, but states can bite, too. We do know that Russia and China, for example, are surveying European and North American cables.

We know China, of course, is investing in 5G, but it is combining that in ways that Germany did as well, with investments in international news networks like the Belt and Road News Network, English language TV channels like CGTN, or the Chinese news agency, Xinhua.

The third lesson, as many of the other witnesses have said, is that we need to think about business models much more than individual pieces of content. It's very tempting to focus on examples of individual content that are particularly harmful, but the reason that those pieces of content go viral is because of the few companies that control the bottleneck of information.

Only 29% of Americans or Brits understand that their Facebook newsfeed is algorithmically organized. The most aware are the Finns and only 39% of them understand that. That invisibility accords social media platforms an enormous amount of power. That power is not neutral. At a very minimum, we need far more transparency about how algorithms work, whether they are discriminatory and so on and so forth. As we strive towards evidence-based policy, we need good evidence.

● (1940)

Fourth, we need to be careful to design robust regulatory institutions. Here, the case of Germany in the interwar period offers a cautionary tale. Spoken radio emerged in the 1920s. Bureaucrats in the democratic Weimar Republic wanted to ensure that radio would bolster democracy in a very new democracy after World War I. As that democracy became more politically unstable, those bureaucrats continually instituted reforms that created more and more state supervision of content. The idea here was to protect democracy by preventing news from spreading that would provoke violence. The deep irony of this story is that the minute the Nazis came to power, they controlled radio. Well-intentioned regulation, if we're not careful, can have tragic unintended consequences.

What does that mean for today? It means we have to democracy-proof whatever the solutions are that we come up with. We need to make sure that we embed civil society in whatever institutions we create.

One suggestion that I made with Fenwick McKelvey and Chris Tenove was the idea of social media councils that would be multi-stakeholder fora and that could meet regularly to actually deal with many of the problems we're describing. The exact format and geographical scope are still up for debate, but it's an idea supported by many, including the UN special rapporteur on freedom of expression and opinion.

Fifth, we need to make sure that we still pay attention to and address the societal divisions exploited by social media. The seeds of authoritarianism need fertile soil to grow. If we do not attend to the underlying economic and social discontent, better communication cannot obscure those problems forever.

Let me then remind you of these five lessons. First, disinformation is also an international relations problem. Second, we need to pay attention to physical infrastructure. Third, business models matter more than do individual pieces of content. Fourth, we need to build robust regulatory institutions. Fifth, we must pay attention to those societal divisions that are exploited on social media.

Attending to all of these things, there is no way they can be done within any one nation; they must be done also through international co-operation. That's why it's such a great honour to have had the chance to appear before you today.

Thank you very much.

The Chair: Thank you, Ms. Tworek.

Next up is Ms. Zuboff.

You, and I with a name like Zimmer, have always been at the end of every list, and you're just about there.

Go ahead, Ms. Zuboff. It's good to have you here.

Ms. Shoshana Zuboff (As an Individual): Thank you so much, Chairman Zimmer.

Indeed, I'm reminded of elementary school tonight.

Of course, you reverse the order tomorrow morning.

The Chair: That's just because I understand.

Go ahead.

Ms. Shoshana Zuboff: It's a lifelong burden.

It's such an honour to be speaking with you tonight, not least in part because I feel this committee right now is our information civilization's best hope for making progress against the threats to democracy that are now endemic as a result of what you've already heard referred to as surveillance capitalism.

I'm so pleased to hear the kind of synergy already in our comments. The themes that the committee has identified to target, the themes of platform accountability, data security and privacy, fake news and misinformation, are all effects of one shared cause. We've heard that theme tonight, and that's such a big step forward. It's very important to underscore that.

I identify this underlying cause as surveillance capitalism, and I define surveillance capitalism as a comprehensive, systemic economic logic that is unprecedented in our experience. I want to take a moment to say what surveillance capitalism is not, because that sets up a set of distinctions we all need to hear.

First of all, and it has been mentioned—thank you, Ben—surveillance capitalism is not technology. It has hijacked the digital for its own purposes. It is easy to imagine the digital without surveillance capitalism. It is impossible to imagine surveillance capitalism without the digital. Conflating those is a dangerous category error.

Second, surveillance capitalism is not a corporation nor is it a group of corporations. There was a time when surveillance capitalism was Google. Then, thanks to Sheryl Sandberg, who I call the typhoid Mary of surveillance capitalism, surveillance capitalism could have been called Google and Facebook. Ultimately, it became the default model for Silicon Valley and the tech sector, but by now this is a virus that has infected every economic sector.

That is why you began with such a startling and important claim, which is that personal data is valued more than content. The reason is that all of these activities, whether we're talking about insurance, retail, publishing, finance, all the way through to product and service, manufacturing and administration, all of these sectors are now infected with surveillance capitalism, so much so that we hear the CEO of the Ford Motor Company, the birthplace of managerial capitalism a century ago, now saying the only way for Ford to compete with the kind of P/Es and market cap that companies like Facebook and Google have is to reconceptualize the company as a data company and stream the data from the 100 million drivers of Ford vehicles. Those data streams now will put them on a par with the likes of Google and Facebook. “Who would not want to invest in us?” he says. We can no longer confine surveillance capitalism to a group of corporations or a sector.

Finally, surveillance capitalism cannot be reduced to a person or a group of persons. As attractive as it is to identify it with some of the leaders of the leading surveillance capitalists or the duopoly, the Zuckerbergs, the Pages, the Brins and so forth, we have blown past that point in our history when we can make that kind of identification.

● (1945)

As an economic logic, which is structure and institutionalize... change the characters, there may be good, independent reasons for changing the characters, limiting their roles and limiting their extraordinary and unprecedented power, but that will not interrupt or outlaw surveillance capitalism.

Having said what it is not, let us just say very briefly what it is. Surveillance capitalism follows the history of market capitalism in the following way. It takes something that exists outside the marketplace and brings it into the market dynamic for production and sale. Industrial capitalism famously claimed nature for the market dynamic, to be reborn as land or real estate that could be sold or purchased. Surveillance capitalism does the same thing, but now with a dark and startling turn. What it does is it claims private human experience for the market dynamic. Private human experience is repurposed as free raw material. These raw materials are rendered as behavioural data.

Some of these behavioural data are certainly fed back into product and service improvement, but the rest are declared as behavioural surplus, identified for their rich predictive value. These behavioural surplus flows are then channelled into the new means of production, into what we call machine intelligence or artificial intelligence. From there, what comes out of this new means of production is a new kind of product—the prediction product. These factories produce predictions of human behaviour.

You may recall a 2018 Facebook memo that was leaked, and we still don't know exactly by whom. That Facebook memo gave us insight into this hub, this machine intelligence hub, of Facebook: FBLearner Flow. What we learned there is that trillions of data points are being computed in this new means of production on a daily basis. Six million “predictions of human behaviour” are being fabricated every second in FBLearner Flow.

What this alerts us to is that surveillance capitalists own and control not one text but two. There is the public-facing text. When we talk about data ownership, data accessibility and data portability, we're talking about the public-facing text, which is derived from the data that we have provided to these entities through our inputs, through our innocent conversations, and through what we have given to the screen. But what comes out of this means of production, the prediction products and how they are analyzed, is a proprietary text, not a public-facing text. I call it the shadow text. All of the market capitalization, all of the revenue and the incredible riches that these companies have amassed in a very short period of time have all derived from the shadow text. These proprietary data will never be known to us. We will never own that data. We will never have access to that data. We will never port that data. That is the source of all their money and power.

Now, what happens to these prediction products? They are sold into a new kind of marketplace that trades exclusively in human futures. The first name of this marketplace was online targeted advertising. The human predictions that were sold in those markets were called click-through rates. Zoom out only a tiny bit and what you understand is that the click-through rate is simply a fragment of a prediction of a human future.

By now we understand that these markets, while they began in the context of online targeted advertising, are no more confined to that kind of marketplace than mass production was confined to the fabrication of the Model T. Mass production was applied to anything and everything successfully. This new logic of surveillance capitalism is following the same route. It is being applied to anything and everything successfully.

● (1950)

Finally, when we look at these human futures markets, how do they compete? They compete on the quality of their predictions. What I have understood in studying these markets is that by reverse engineering these competitive dynamics, we unearth the economic imperatives that drive this logic. These economic imperatives are institutionalized in significant ecosystems that thread through our economy, from suppliers of behavioural surplus to suppliers of computational capabilities and analysis, to market makers and market players.

These imperatives are compulsions. From these imperatives, every single headline—we open the paper every day and see a fresh atrocity—can be predicted by these imperatives. It began with economies of scale. We need a lot of data to make great predictions. It moved on to economies of scope. We need varieties of data to make great predictions. Now it has moved into a third phase of competition, economies of action, where the most predictive forms of data come from intervening in human behaviour—shaping, tuning, herding, coaxing, modifying human behaviour in the directions of the guaranteed outcomes that fulfill the needs of surveillance capitalism's business customers.

This is the world we now live in. As a result, surveillance capitalism is an assault on democracy from below and from above.

From below, its systems globally institutionalize systems of behavioural modification mediated by global digital architectures—our direct assault on human autonomy, on individual sovereignty, the very elements without which the possibility of a democratic society is unimaginable.

From above, what surveillance capitalism means is that we now enter the third decade of the 21st century. After all the dreams we held for this technology, which Ben has described to us, we enter this third decade marked by an asymmetry of knowledge and the power that accrues to that knowledge that can be compared only to the pre-Gutenberg era, an absolutist era of knowledge for the few, and ignorance for the many. They know everything about us; we know almost nothing about them. They know everything about us, but their knowledge about us is not used for us, but for the purposes of their business customers and their revenues.

To complete, it is auspicious that we are meeting tonight in this beautiful country of Canada, because right now, the front line of this war between surveillance capitalism and democracy is being waged in Canada, specifically in the city of Toronto. Surveillance capitalism began with your online browsing and moved to everything that you do in the real world. Through Facebook's online massive-scale contagion experiments and Google-incubated Pokémon GO, it experimented with population-level herding, tuning and behaviour modification.

Those skills, by the way, have now been integrated into Google's smart city application called Waze. But the real apple here, the real prize, is the smart city itself. This is where surveillance capitalism wants to prove that it can substitute computational rule, which is, after all, a form of absolutist tyranny, for the messiness and beauty of municipal governance and democratic contest.

● (1955)

The frontier is the smart city. If it can conquer the smart city, it can conquer democratic society. Right now, the war is being waged in Toronto. If Canada gives Google, that is, Alphabet—Sidewalk Labs now goes out of its way to claim that it is not Google—Toronto, a blow will be struck against the future possibilities of a democratic society in the 21st century.

Thank you for your attention. I hope to return to this discussion tomorrow with the rest of the testimony.

Thank you so much.

The Chair: Thank you, Ms. Zuboff.

Last, I will go to Maria Ressa. She's coming all the way from Manila in the Philippines.

Go ahead, Ms. Ressa.

Ms. Maria Ressa (Chief Executive Officer and Executive Editor, Rappler Inc., As an Individual): Good morning.

First of all, what a privilege it is to be in front of you and to listen to everyone. Take everything that you've heard, especially what Shoshana just said.

I'm living this stuff right now. I've been a journalist for more than 30 years, and in the last 14 months, I've had 11 cases, five against me by the government. I've had to post bail eight times in a little over three months, and I've been arrested twice in five weeks. All of this stuff, bottom up.... I call that astroturfing on social media bottom-up information operations that are going down, and then you have top down, which again was described for you much more fully earlier.

I'm going to keep it short because I'll give you a formal presentation tomorrow. I think that, in the end, it comes down to everything that you have heard. It comes down to the battle for truth, and journalists are on the front line of this, along with activists. We're among the first targeted. The legal cases and the lobbying weaponized against me came after social media was weaponized. So, with regard to this battle for truth, at no other time do we really know that information is power. If you can make people believe lies, then you can control them, and that's aside from the commercial aspects of it. We're talking about information as a means to gain geopolitical power. If you have no facts, then you have no truth. If you have no truth, you have no trust.

We've seen that erosion. We first, at Rappler, were a start-up that really looked at information cascades, social networks, family and friends. Social media are your family and friends on steroids, so we looked at how information cascaded. What I'll show you tomorrow is the data that shows you exactly how quickly a nation, a democracy, can crumble because of information operations. If you say a lie a million times, it is the truth. There is this phrase “patriotic trolling”. It is online state-sponsored hate that targets an individual, an organization or an activist, pounding them to silence, inciting hate. We all know that online hate leads to real world violence.

We're the cautionary tale. I've had as much as 90 hate messages per hour. My nation has moved in three years' time from a very vibrant democracy where social media for social good was really used—we lived it. I believed we were.... My organization was one of the ones that worked very closely with Facebook, and then to see it weaponized at the end of 2015 and 2016.... It wasn't until after President Duterte took office in July 2016, the beginning of the drug war. The first targets were anyone on Facebook who questioned the numbers of killings. The UN now estimates that 27,000 people have been killed since July 2016. It's a huge number.

I'll end by saying that tomorrow I will give you the data that shows it. It is systematic. It is an erosion of truth. It is an erosion of trust. When you have that, then the voice with the loudest megaphone wins. In our case, it's President Duterte. We see the same things being carried out in the United States. Whether it's Trump, Putin or Duterte, it's a very similar methodology.

I'll end with this and just say thank you for bringing us in. I mean, what's so interesting about these types of discussions is that the countries that are most affected are democracies that are most vulnerable, like ours here in Southeast Asia, in the global south. Every day that action is not taken by the American tech platforms, the social media platforms that should have American values.... The irony, of course, is that they have eroded that in our countries.

There is some action that has been taken. I will say that we work closely with Facebook as a fact-checker, and I've seen that they're looking at the impact and that they have been trying to move at it. It has to move much faster.

Here's the last part of this: If they're responding to political situations in the west, that normally leads to neutral responses. Neutral responses mean that, in the global south, people will die and people will get jailed. This is a matter of survival for us.

Thank you.

● (2000)

The Chair: Thank you, Ms. Ressa.

That pretty much brings us to the end of our testimony for this evening.

We're going to Room 225A down the hall to meet more informally and to be able to ask you questions directly. I'm sorry again, Ms. Ressa, that you're not able to be here, but again the idea tonight was to get the conversation going and that will continue over there.

I want to remind everybody we are going to start crisply with testimony at 8:30 tomorrow morning, so I challenge you to be here when you can. I am going to be much more limiting. I gave some latitude with time tonight. Folks on the committee, tomorrow it's five minutes each for questioning. Again we look forward to the testimony.

We won't hear some of you again, but we thank you for making the special trip to be part of this panel tonight, and we look forward to this conversation continuing. Regardless that the Wednesday meeting ends at noon, the conversation will continue on how to make our data world a better place.

We'll see you just down the hall.

The meeting is adjourned.