HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 121 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, October 18, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, October 18, 2018

● (1115)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): I apologize for the late start.

We're joined by the Bank of Canada, the Competition Bureau and CSE today. I thank all of you for attending.

We'll start with a presentation from the Competition Bureau.

[*Translation*]

Mr. Anthony Durocher (Deputy Commissioner, Monopolistic Practices Directorate, Competition Bureau): Mr. Chair, Thank you for the opportunity to appear today.

I am Anthony Durocher, Deputy Commissioner of Monopolistic Practices at the Competition Bureau and I am joined by my colleague Alexa Gendron-O'Donnell, Associate Deputy Commissioner of the Bureau's Economic Analysis Directorate.

The Bureau is an independent law enforcement agency that ensures Canadian businesses and consumers prosper in a competitive and innovative marketplace.

The Bureau administers and enforces Canada's Competition Act, which involves investigating and addressing abuses of market power, anti-competitive mergers, price-fixing and deceptive marketing practices.

Competition law enforcement requires more than theory. Evidence-based enforcement is at the heart of what the Bureau does and this requires that our decisions be based on credible evidence that can withstand judicial scrutiny.

It is also important to recognize that we are enforcers, not adjudicators. The Competition Act requires us to meet several thresholds and standards, such as proving there has been a significant harm to competition.

Regardless of if we want to bring a case forward, we are guided by the decisions of the Competition Tribunal and courts.

[*English*]

It is difficult to turn on the television or read the news without seeing the increasing role of data in our economy. The power that data now represents, and the control that digital platforms have over it, deserves careful consideration. The bureau recognizes its important role in this area and strives to be a leader through both its enforcement work and its policy work, both of which we plan to discuss today.

We understand that this committee is particularly focused on privacy. It is important for me to say from the outset that safeguarding privacy is not an explicit goal under the Competition Act, so our role is limited in this regard. However, there are two ways privacy can be relevant to our work. First, if companies compete to attract users by offering privacy protection, then this dimension of competition can be a relevant factor in reviewing anti-competitive activity. Second, if companies mislead consumers about whether and how their data will be used, this may also raise concerns under the Competition Act.

There are many obvious benefits associated with the collection and analysis of data, particularly for driving innovation, but there are also risks. The bureau has a mandate to safeguard competition in the digital economy, and we continue to prioritize this work. However, it is important to acknowledge that competition law has its limits. It is not a cure-all for the broader threats that data and data-driven platforms may pose for society, such as breaches of privacy, election tampering or manipulation of public opinion. These risks go beyond our legal mandate. Nevertheless, we are happy to bring our competition expertise to bear on this important discussion, as these issues are cross-cutting and will benefit from collaboration across government to protect Canadians.

A little over a year ago, the bureau published a comprehensive white paper entitled, “Big data and Innovation: Implications for Competition Policy in Canada". The purpose of this paper was to engage with stakeholders by prompting a discussion on how the emergence of big data should affect competition law enforcement.

Following an extensive consultation, the bureau found that there's no need for hasty moves in this area. The current framework is up to the task, but our tools must evolve to deal with the complex issues arising from digital platforms, such as those that monetize user data through advertising by offering free services to consumers.

● (1120)

A recurring concern we hear about is the large and growing size of some tech firms, but big doesn't necessarily mean bad. Becoming big is the reward a firm could get for successfully introducing an innovative product. We should not punish this success. Only when we find evidence that a big firm is engaging in harmful anti-competitive conduct should we intervene.

It is important to find the right balance between preventing any competitive behaviour that harms Canadian consumers and avoiding undue over-enforcment and the inadvertent harm this may cause to innovation and the economy. Some of the issues that we have heard about relating to the digital economy and our monitoring include firms buying emerging competitors or excluding disruptive ones; firms that may use artificial intelligence or algorithms to collude and fix prices; and firms misleading consumers about whether and how their data will be used. If we find evidence that any of these practices violate the Competition Act, the bureau will act to protect Canadians.

We have already conducted several notable investigations in the digital economy, including against Google over an alleged abuse of market power related to its search engine, and the Toronto Real Estate Board, or TREB, over its real estate data.

Our case against TREB is a great example. We were able to stop TREB from withholding its real estate data from agents who wanted to offer innovative online services to homebuyers and home sellers. This case exemplifies how we are ensuring that Canadian consumers benefit from the innovation happening in the digital economy.

We welcome the opportunity to discuss the bureau's white paper, as well as these recent cases, in greater detail during the question and answer period.

[*Translation*]

The digital economy is a top priority for the Bureau. We will continue to monitor the online marketplace, including the conduct of large tech firms.

We will also continue to work closely with our domestic and international partners and carefully review the actions taken by our international counterparts. However, laws and competitive dynamics may differ significantly between countries, and we must remain mindful of that.

The Bureau also encourages all Canadians to reach out to us if they have any evidence of violations of the Competition Act.

Before fielding your questions, I would note that the law requires the Bureau to conduct investigations in private and keep confidential the information we have. This obligation may prevent us from discussing some past or current investigations.

We appreciate the opportunity to appear before you to discuss our work and look forward to your questions.

Thank you.

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much. That's much appreciated.

Our next presentation will come from the Communications Security Establishment.

You have 10 minutes.

Mr. Dan Rogers (Deputy Chief, SIGINT, Communications Security Establishment): Thank you, and good morning, Mr. Chair and members of the committee.

My name is Dan Rogers, and I'm the deputy chief of foreign signals intelligence at the Communications Security Establishment. I am responsible for CSE's foreign signals intelligence program. I'm joined today by my colleague André Boucher, the assistant deputy minister of operations at the Canadian Centre for Cybersecurity.

The Canadian Centre for Cybersecurity, which is a part of CSE, is Canada's national authority on cybersecurity and cyber-threat response. It's a pleasure to appear before you as you continue your study.

With regard to the incident involving Cambridge Analytica and Facebook, CSE does not have a mandate to regulate social media, nor is it a law enforcement agency. We have no oversight role with respect to these companies. We do, however, have a role in identifying and helping protect against cyber-threats to Canada's democratic process. Therefore, I would like to focus my remarks on these threats and how they can be mitigated through good cyber and physical security.

I also hope to leave you with a better sense of what CSE does and how we have changed as an organization since CSE officials last appeared before this committee in 2017.

CSE is Canada's national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance. I would like to emphasize that CSE only directs its signals intelligence activities at foreign communications. CSE is prohibited by law from directing its activities at Canadians anywhere or at anyone in Canada.

CSE operates at the cutting edge of today's threat environment. Whether providing intelligence on foreign-based terrorism or threats to Canadians abroad, or defending against cyber-attacks, CSE helps to ensure Canada's prosperity, security and stability.

More recently, CSE was asked to assist the Minister of Democratic Institutions with her mandate to lead the Government of Canada's efforts to defend the Canadian electoral process. Specifically, the mandate letter for the Minister of Democratic Institutions directed that she ask CSE to analyze risks to Canada's political and electoral activities from hackers and release this assessment publicly, and to offer advice to Canada's political parties and Elections Canada on best practices when it comes to cybersecurity.

In response, we released a report on cyber-threats to Canada's democratic process in June 2017. While the report is unclassified, key judgments in the assessment rely on multiple sources including classified information from CSE's unique cybersecurity and foreign intelligence expertise. CSE examined cyber-threat activity against democratic processes across Canada at the federal, provincial and territorial, and municipal levels and around the world. The report examined the types of threat actors involved, the targets they are likely to select and the methods they may use to target their victims.

CSE assessed that in the 2015 Canadian federal election, Canada's democratic process was targeted by low-sophistication cyber-threats likely perpetrated by hacktivists and cyber criminals. These activities had no effect on the results of the election and no impact on the privacy of Canadians. CSE has assessed that, at the federal level, political parties and politicians and traditional and social media are more vulnerable to cyber-threats than election activities themselves.

Consistent with the increasing cyber-threat activity against democratic processes worldwide, we expect to see multiple hacktivist groups deploying cyber capabilities in an attempt to influence the democratic process during the 2019 federal election. These will likely be low-sophistication activities, but will be well planned and will target more than one aspect of the democratic process.

CSE has been asked to continue this analysis and expects to release an update to the 2017 report.

While offering mitigation advice was outside the scope of the threat report, to respond to Minister Gould's second request of CSE, we have held briefings with political parties, provincial and territorial clerks, and Elections Canada to offer best practices when it comes to cybersecurity.

Our key message in all of these briefings is that, while system safeguards are expected to curtail most suspected malicious activity, we cannot rely solely on technical safeguards. Users must also be diligent and have good cybersecurity habits in order to stop the threats of today and to stay ahead of the threats of tomorrow.

CSE has made available on its website several documents, the "Top 10 IT Security Actions", "Cyber Hygiene", "Mobile Security" for IT enterprise, and other resources with user best practices. We'd be happy to speak to any of these in greater detail during the questions and answers.

● (1125)

Cybersecurity is a team sport. We'll continue to work with Elections Canada to ensure that the electoral process is secure and remains a trusted aspect of our democratic process.

CSE will work with Minister Gould and other stakeholders, if requested, to advance the goal of protecting Canada's democratic institutions and electoral processes from cyber-threats.

On October 1, the Minister of National Defence announced the launch of the cyber centre, Canada's national authority on cybersecurity and on cyber-threat response. The cyber centre, housed at CSE, brings together cyber expertise from Public Safety Canada, Shared Services Canada and CSE all under one roof. A unified government source of expert advice and guidance for the private sector, critical infrastructure owners and operators and all Canadians, the cyber centre will help ensure a safe and secure cyberspace.

This newly established centre will also enable better coordination of efforts in the protection of Canada's democratic institutions from cyber-threats. This includes the period preceding the 2019 federal election.

Again, thank you for inviting us here today. We look forward to answering your questions.

● (1130)

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

Our last presentation will come from Eric Santor from the Bank of Canada.

Thanks very much for joining us today. You have 10 minutes.

Mr. Eric Santor (Managing Director, Canadian Economic Analysis, Bank of Canada):

Good day, Mr. Chairman and committee members, and thank you very much for the invitation to be here.

As the managing director of the Canadian economic analysis department of the Bank of Canada, I'm happy to present our views and observations regarding the declining competition in advanced economies. I'll also address the implications for both competition and the longer-term dynamism of the economy related to the emergence of large tech firms as well as the growing importance of big data.

Understanding the impact of digitalization on the Canadian economy is crucial as we seek to achieve our objective of low, stable and predictable inflation. The Bank of Canada does not have a regulatory role with respect to the privacy of citizens' data so I trust you will understand that I will not be able to address the privacy implications of these issues.

The Canadian economy is digitalizing rapidly. Digital disruption is expected to be positive for economic progress overall. New firms are being created and existing ones are being transformed as new technologies change the way businesses operate. For consumers, digitalization means that households can purchase a seemingly ever-widening range of goods and services 24-7 from around Canada and from around the world.

[*Translation*]

Digitalization will contribute to higher productivity, and hence higher living standards, in the coming years and decades.

There is a lot of concern about the rise of the robots and how they could take away people's jobs. Naturally, we tend to focus on these initial effects. But we also need to be mindful that it takes a long time to fully replace a worker with a robot.

[*English*]

Still, there is no doubt there will be disruption for some, and there is time for society to adjust. People whose jobs are affected will need support. Job training and a strong safety net are key.

We must also remember that digitalization is creating new kinds of jobs and will create some that haven't even been imagined yet. These new jobs will help the economy grow. New jobs mean new incomes, which will be spent not just in the digital economy but across the whole economy, with benefits for workers in traditional jobs too.

One of the driving technologies of digitalization is the application of artificial intelligence and machine learning in conjunction with big data to a wide range of business applications. AI and ML increase firms' productivity in three major ways. First, AI and ML help companies make better products and improve their customers' experiences. Second, they help develop products and services more efficiently and more quickly. Finally, they help firms reach new markets and customers.

[*Translation*]

There are practically countless examples of such applications.

They include farmers using GPS autopilots to drive their tractors and optimize fertilizer and pesticide use; robots working on factory floors and in warehouses, "driving" forklifts to move goods and digitally track them from supplier to retailer; Al offering up suggestions for products or services you may wish to buy; and having chatbots and robo-advisers standing ready to answer your questions when you visit websites.

[*English*]

By implementing AI and ML with big data, firms can gain a competitive advantage, ultimately through offering a better product or service at a lower price. One of the features of AI and ML, big data and network effects is that there are often significant benefits in being a first mover. In fact, market concentration happens quite naturally in industries with prominent network effects and other scale economies.

In the current environment, this dynamic can lead to the creation of superstar firms. These firms tend to have fewer employees than conventional companies and they often earn impressive monopoly profits.

What is new is that the winner-takes-all effect is magnified in the digital economy because user data has potentially become another source of monopoly power. Data from a large network creates a formidable barrier to entry in some cases. Another barrier to entry can come from firms using the position as gatekeepers of crucial online services to impede their competitors and thwart innovation. In this context, we believe competition policy can be modernized appropriately to help ensure that benefits of digitalization are fully realized.

What do we know? What evidence do we have on the issue of market concentration, markups and prices?

In recent years, economists have paid considerable attention to the secular rise of market concentration in advanced economies. In particular, models have been developed that tie this rise to digitalization. Specifically, these firms are able to capture an increasingly large share of the market because of technological advances, such as AI and ML with big data, thereby increasing concentration. They also have a high share of profits, which can lead to a fall in the labour share of income.

Overall, most industries have seen an increase in their concentration over the last 15 years. Although the evidence is not conclusive, a broad increase of industry concentration across countries suggests that technological change, that is, digitalization, rather than country-specific factors, is perhaps the main driver.

One concern in an environment dominated by superstar firms is that those firms have more power when setting prices, which could lead to an increase in prices. That's why economists have also been looking at the secular rise in market power of firms as measured by markups. For example, researchers documented a rise in average markups in the U.S. from 1980 to 2014. They also found that global markets have risen as well. This increase is also observed in Canada. For Canada, they document a very similar overall trend to the U.S., a finding confirmed by the IMF. This suggests that market power's been rising in many countries over the past few decades.

The next question is whether digitalization has affected consumer prices. This is often referred to as the “Amazon effect”, where competition from digital retailers results in lower prices. It may appear inconsistent that digitalization can lead to both higher markups and lower prices. However, it is simply that the benefits of technology partly go to the customer in the form of lower prices, but also to the firm in the form of higher markup over lower cost.

While the direct evidence of the impact of digitalization on inflation is mixed, it does tend to point to downward pressure overall. In a research paper published last year, bank staff found that the direct evidence pointed to a small negative impact of digitalization on inflation. That is, digitalization was weighing on price increases rather than feeding them. Evidence using online prices data, such as the Billion Prices Project, is mixed. Some find that online prices tend to behave similarly to bricks-and-mortar store prices, while others find big effects on inflation year over year on the downward side. Most of us are familiar with why this might be happening—our ability to check competitor's prices using our smart phones before we head to the checkout.

Finally, when using the framework upon which the bank's main economic models are built to assess the channels through which digitalization may affect inflation, we find that most developments associated with digitalization would put downward pressure on inflation.

Overall, the impact of digitalization on market concentration, and hence competition, remains an open question. The bank will continue to examine the impact of digitalization on the Canadian economy as we pursue our objective of promoting the economic and financial welfare of Canada.

● (1135)

[*Translation*]

Thank you once again for the invitation to appear.

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you all for your presentations.

We'll go to our seven-minute round.

The first seven minutes go to Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning.

Thank you all for being here.

I can't resist asking this question of Mr. Santor.

Inflation might not be a really trendy topic, but I know that central bankers worldwide have pursued an inflationary rate target of being less than 2%. Now you're bringing retailers into the mix. They have two models: bricks-and-mortar and online. There is a price differential. I've seen it myself when I go to the store. Some of these products are not calculated in your consumer price index, so how do you make an accurate measurement of what's actually happening in the marketplace? The marketplace itself has changed.

Mr. Eric Santor: Our mandate is to target inflation at 2% with a range of 1% to 3%. The CPI itself is constructed by Statistics Canada, so you would need to direct your question towards them to ask whether or not the CPI is reflecting these developments.

I know that they are aware of this issue. That is certainly on their agenda.

Mr. Raj Saini: Does it not make it difficult for you, then, when you do your assessments?

Mr. Eric Santor: What we do observe is the CPI, and that does have both online and bricks-and-mortar prices in it. We observe this. Since we know that online prices would be putting downward pressure on bricks-and-mortar prices, that would be already embedded in the CPI as that competition effect feeds through. When we talk to [*Technical difficulty—Editor*] in our surveys, they tell us that, yes, they are feeling downward pressure on their prices from online competition, so that is captured to some extent.

Mr. Raj Saini: Okay.

Mr. Rogers, I'm going to spend some time with you this morning.

How would you assess the current threat level to the Canadian democratic process, specifically in terms of the 2019 election? In your opening comments, you talked about 2015, when there was low-level activity, but now we're going into 2019 and obviously there are more actors on the stage. How would you assess our threat level right now?

Mr. Dan Rogers: I'm happy to take the question, and thank you. This is something that the last report touched on. I know that our cyber centre is preparing a new report that will touch on that topic.

Maybe I can ask André to pick that up.

● (1140)

[*Translation*]

Mr. André Boucher (Assistant Deputy Minister, Operations, Canadian Centre for Cyber Security, Communications Security Establishment): All right.

We indicated in our June 2017 report that we were expecting an increase in the use of cyberspace and that various types of threats would increase as a result.

An update to that report is expected early next year, but I'm going to tell you now what you can expect from it.

Threats have indeed increased, but the main difference is the speed at which threat levels have risen. We were expecting them to rise, but it's happened more quickly. This also applies to Canada. No one will be surprised given what's happening internationally.

[*English*]

Mr. Raj Saini: That leads to my second question. Is there any risk that Canadian voter lists or those of Canadian political parties could be compromised? We saw an example of that in the 2016 election with the DNC and the Clinton campaign. Where are we with that now?

[*Translation*]

Mr. André Boucher: Thank you for that question, Mr. Saini.

We're really on the lookout because we know what's happened internationally. We began working with the Elections Canada people early on to ensure that the networks, systems and procedures put in place were equal to the task of handling the rising threats I just mentioned. I'm entirely satisfied that the measures, processes and technologies put in place will help Canada tackle those threats to voter lists.

[*English*]

Mr. Raj Saini: I don't want to mention any names, but obviously there are certain state actors around the world that have been known to engage in activity to disrupt elections. One of the things that concerns me is that sometimes the state actors don't come forward themselves. They have other entities, other organizations and other groups that act on their behalf to disrupt not only elections but other activities in other countries.

I don't want you to compromise your tactics of how you deal with this, but how do we deal with that? It seems to me that it's a problem. There's a great proliferation. How do we deal with that? You have certain entities that you are aware of and you're known to be aware of those entities, but then they have so many sub-entities that work in an arm's-length process and can contribute to the destruction of a campaign. In what way will you manage that?

[*Translation*]

Mr. André Boucher: We ranked threats by category in our June 2017 report.

Here's an example that goes to your question. Synchronization and subcontracting do occur between states and perhaps between criminal entities.

In reality, we constantly monitor all threats. Threat prevention and detection measures and ways to react to threats are based on each group, not on a more dominant group. We monitor all groups. We, of course, observe any interconnections that didn't previously exist. People employed by others become threats without knowing it. Some firms even believe they're operating entirely legally in executing contracts, but are in fact being used to conduct research for others. This phenomenon is real, and we're aware of it. We're doing what we can.

Mr. Rogers, do you want to add something on the subject of threats?

[*English*]

Mr. Raj Saini: Mr. Chair, how much time do I have?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): You have 40 seconds.

Mr. Raj Saini: This is my last question, as I'm running out of time.

Obviously, now there are different ways of communicating with the public. We use social media platforms like Facebook and Twitter.

Do you work with them in any concerted way to make sure that if there are threats emanating, they can be shut down really quickly so they don't proliferate to an extent which can have a material impact on an issue or a campaign, whether it be bots or trolls or misinformation that's put out there? Do you have a relationship with them? I think that would be critical to making sure that misinformation is not being spread online.

[*Translation*]

Mr. André Boucher: Absolutely. To protect Canadians, the Canadian Centre for Cybersecurity uses a cooperation model, under which all stakeholders work together. It involves the user, as Mr. Rogers said, the manufacturer, the people who produce the source codes and the software, right up to the Internet service provider. The provider also has a social responsibility, and we treat it as a Canadian business. If we discover something unusual, we immediately advise it of the fact. If it hasn't already detected it, it will be very receptive and will immediately take measures.

● (1145)

[*English*]

Mr. Raj Saini: Thank you.

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

I understand that Mr. Kent will be leaving us shortly, but we'll give him seven minutes just before he does.

Hon. Peter Kent (Thornhill, CPC): I appreciate that, Chair. Thank you very much.

Thank you to all for appearing this morning.

I recognize that the Competition Bureau and the bank have only peripheral suggestions that might be applied in the recommendations we make to government on completion of this report on the digital vulnerability of the Canadian electoral system, or threats to the Canadian electoral system. Therefore, I'd like to direct all of my time to the CSE witnesses today.

As a politician, I participate in social media almost entirely for political benefit, and there are significant benefits to using Facebook, Instagram and other social media—Twitter.

This week the digital threat was brought home to me when my Instagram account was seized by someone from outside of the country. My Facebook account was hacked and took some time to be recovered.

It brought to mind the so-called Beyoncé trick, which previous witnesses have spoken to before the committee. In the United States, in the last federal election, a Facebook fan page was created paying tribute to Beyoncé, which accumulated millions of followers. Then, in the final days of the election campaign—and this was set up, we understand, by Russian players at one level or another—messaging went out which, in the end it has been concluded, was aimed at discouraging black voters from voting in that campaign, or in some of the campaigns.

We asked one of our previous witnesses, Dr. Ben Scott, about how Canadians might protect themselves from the sort of Trojan Horse social media time bomb that was set to go off in the decision-making period in an election campaign. He suggested that agencies like the CSE would be playing what he called "red teaming", Cold War game playing, in trying to anticipate threats, how one would respond to threats, how one would see this as a fraudulent attempt to interfere with the election process. He essentially said that security agencies have an ability—and I recognize you have no authority over social media—and certainly American security agencies have an ability, to see foreign intervention or foreign players in the social media sphere.

I'm wondering if you could address what the CSE is doing in that area.

Mr. Dan Rogers: Certainly. Thank you for the question.

I'll answer from the foreign intelligence perspective, which is in my domain. Then I'll invite André to talk to some of the guidance we provide to Canadians to deal with that sort of issue.

As a foreign intelligence-mandated organization, we do track targets on the global information infrastructure, which includes social media. If we have intelligence priorities from the government, which would include things like looking at foreign nations that would have an interest in disrupting our electoral systems, we would look anywhere on the global information infrastructure to identify what those activities, capabilities and intentions of those foreign states are.

I can't in this setting speak to the details of how we do that, but I can definitely say that it is an active part of our role to observe that activity to the extent that we can. Then we roll that up into foreign intelligence products to provide to our partners in the government, and to André's team, which form the basis of some of their cybersecurity advice and work with those who may be affected by these activities.

André, do you wish to speak to that?

Mr. André Boucher: Absolutely.

Of course, we already provide advice and guidance on how to secure the devices, the utilization of devices, and so on and so forth. I'll leave that aside. Just to follow up on Dan's point, when the teams are informed that there's activity in a foreign space, I think it goes back to the previous question. There's the opportunity for us. We would tell the user to contact the company and let them know, but because we have these partnerships as well, we would also inform the company that we're seeing evidence that something is wrong with their service delivery and that perhaps they might want to turn their attention to it. What we try to do is get this information in the right way to those who can actually do something about it.

● (1150)

Hon. Peter Kent: The study we've conducted this year, since the Cambridge Analytica, Facebook, AggregateIQ scandal broke, involves a significant amount of testimony that says that the big data companies have been more preoccupied in developing their business plans and profits and competition rather than on the protection of privacy.

In your experience in dealing with the big data companies, have they been co-operative in terms of responding to your advice? You don't necessarily have to name the companies, but for our viewing audience, I'd suggest Facebook, Amazon, Google and so forth.

[*Translation*]

Mr. André Boucher: The very short answer is yes, but I'll nevertheless give you a little context.

You have to be pragmatic. I meet with corporate boards and presidents to discuss the idea of introducing security measures, whether it be to protect privacy or to ensure overall security, to preserve the confidentiality, integrity and availability of their networks.

Service providers must strike a balance between the profitability and the security of their product. Don't be naive. When I ask people from companies in all fields to ensure their product or service is secure, I have to give them convincing arguments for them to tighten up their security measures. Having relevant information on a given threat helps us convince them. In fact, we have a lot of success in this area.

[*English*]

Hon. Peter Kent: Thank you very much.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): The next seven minutes will go to MP Mathyssen.

Ms. Irene Mathyssen (London—Fanshawe, NDP): Thank you very much, Mr. Chair.

Witnesses, thank you very much for being here.

This is a wealth of information, and I truly appreciate it. Some of it is a tad terrifying, but I'm sure that we'll sift through that and determine how best to tackle this very large question.

It's probably Mr. Durocher who could best answer this question. Yesterday there was a lawsuit filed against Facebook. The allegation is that they manipulated the numbers in regard to how many people were watching videos on their network. Of course, there are implications for those who work in media, the people who write for media outlets, and also advertisers.

I wonder if you would regard this as an abuse of market power. Does it have broader implications in regard to that question?

Mr. Anthony Durocher: Thank you very much for the question.

Canada's Competition Act, in terms of the abuse of market power provisions, is really aimed at dominant companies that engage in action that harms the competitive process and that is intended to keep competitors out of the market from competing on the merits with them. An instance of a firm that may be engaging in conduct that would be tantamount to exercising market power, such as raising prices, does not necessarily fall offside of the Competition Act. It's really geared towards protecting the competitive process. In the context of conversations around the large tech companies, really our role is to ensure that the competitive process is protected and that companies are afforded the opportunities to compete with Facebook on the merits of their products and services.

Ms. Irene Mathyssen: Obviously, Facebook benefits by the number of people watching and using it in terms of selling advertising. It seemed interesting in regard to this lawsuit, so thank you for that.

This question is for the Bank of Canada.

I wonder whether the bank has any concerns about concentration of superstar firms. You described that. Most of these are in the United States. Does this impact the ability of Canadians to build first-rate, domestic, digitalized business space? Apart from that, what's the impact on retailers?

● (1155)

Mr. Eric Santor: Thank you very much for the question. It's a good question.

What we're seeing right now in the Canadian economy is there's a lot of activity in the digital economy. While we don't have an explicit measure of the digital economy, the things that we do look at show there's very robust growth. Taking one measure, for example, if you look at GDP by industry, there's a category called computer systems design and related services. It's been growing more than 7% a year for the last five years. In value-added space, it's as big as autos and aerospace combined. So there's very rapid growth, a lot going on.

If you look more anecdotally in centres like Toronto, Montreal, the Waterloo corridor, Edmonton and other places, there's a lot of digital activity, a lot of investment going on in IP and research and development. Also, this has attracted the interest of large players to bring FDI into Canada, with them locating here, to benefit from the talent pool we have in terms of big data, AI and ML and a lot of artificial intelligence. By one metric, Canada has the third largest number of researchers in AI and ML, so we're well positioned to take advantage of this, and we see this as a really strong driver of the Canadian economy right now.

Ms. Irene Mathyssen: So the brain drain that we always seem to fear is not a reality. We are, indeed, attracting and keeping highly skilled professionals.

Mr. Eric Santor: Yes. It's a very competitive job market for data scientists and people who are conversant in AI and ML, but we're very well positioned. We produce a lot of talent ourselves, and we are attracting talent as well.

Ms. Irene Mathyssen: Okay. Thank you very much.

Mr. Durocher, the European Union has taken the proactive approach to antitrust enforcement against data-opolies such as Google. I wonder if you can explain the difference between the Canadian and the European approaches to that.

Mr. Anthony Durocher: Sure. That's an important thing, and I can tell you the Competition Bureau is very closely monitoring what is going on in Europe and elsewhere around the world. When we look at these large companies, this is a global issue and it's not Canada specific. An important thing is that we work together. We're aware of what is going on elsewhere, what tools they're using, to make sure that here in Canada we're using cutting-edge methods. It's no secret that the European Union has brought two cases against Google. There's also a recently announced investigation against Amazon. The German competition authority has an ongoing case against Facebook as well.

What I can tell you is the important thing to be mindful of is the difference not only in competitive dynamics between Europe and Canada, but also in the laws. Canada's abuse of dominance law is well established since 1986, with jurisprudence about what are the elements that need to be met to bring a case. All the work that we do is really principled, evidence-based enforcement. Our decisions in Canada are really informed by the evidence at hand and any harm to the Canadian market. With respect to Google in particular, in 2016 we closed a very lengthy three-year investigation against Google for some of its practices, and there was a commitment provided by Google for a competition issue that we had identified. But going forward, we are closely monitoring and working with our international counterparts to ensure that here in Canada we are staying on top of things.

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

Our last seven minutes go to Mr. Picard.

[*Translation*]

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

My question is for the people from the Competition Bureau.

If Facebook handed over a significant amount of private data to a party for some kind of analysis and that party entered into an agreement with a third party over which we had no control, information would be scattered around without any control. Would the third party that got its hands on that metadata under a secret or even criminal agreement—it would have no right to sell the data but would nevertheless do so—be engaging in unfair competition?

● (1200)

Ms. Alexa Gendron-O'Donnell (Associate Deputy Commissioner, Economic Analysis Directorate, Competition Promotion Branch, Competition Bureau): Thank you very much for your question.

Allow me to continue in English.

[*English*]

The Competition Bureau, in addition to the sections that my colleague spoke about, also has what we call a section for false or misleading representation. When I talk about representation here, I mean marketing material, online advertisements, social media messages, even terms and conditions. The big thing under the Competition Act is that the general impression you are conveying has to be truthful. There has to be truth in advertising. When it comes to promoting your business interests or collecting consumer information, you must be truthful. That is the section of the act that would be engaged when any company is thinking about making some kind of representation to consumers, whether it's to sell them a product or to give them what I would call a free product in exchange for their information. You must abide by the act in those cases.

[*Translation*]

Mr. Michel Picard: A social network that asks me for information for sign-up purposes is very transparent. It clearly states in its conditions that its partners and it are entitled to use my data. That's quite transparent, but I have no idea who its partners are.

Ms. Alexa Gendron-O'Donnell: That's correct. I'll continue my answer.

[*English*]

Really, it is about the misleading advertising provisions. We encourage companies to be clear, but the biggest thing is to not mislead. You cannot tell consumers that you are going to do one thing and then do another. Really, the competition provisions are about ensuring that there is truthful advertising to these customers, so that customers know, when they are about to purchase a product or give information, that there may be a possibility that it goes to a third party, or that it is used elsewhere.

Mr. Michel Picard: They don't, however, take responsibility for the partner's business. They don't take responsibility for what the partner is going to do with the data they are exchanging. If I agree to exchange my social media with a partner, and the partner does something totally different, I'm going to address it to the CSE afterwards. But if it's all written in the contract and it's transparent and there's no misleading, then it's just omission. Is "omission" different from "misleading", as you see it?

Ms. Alexa Gendron-O'Donnell: The big thing with the commission is just ensuring that the representation made to the customer is truthful. That is really the core of the law here. Certainly, if that secondary company at any point makes a representation to consumers, they absolutely have to ensure that it is truthful.

Mr. Michel Picard: Regarding CSE, we have in mind that a third party in a scenario has millions and millions of data. You mentioned that the threat is increasing, especially for 2019. Can you identify the nature of the threat? Is it more individuals, institutions or associations, corporations or government, or is it all of the first three under a foreign government umbrella?

Mr. Dan Rogers: [*Inaudible—Editor*]

[*Translation*]

Mr. André Boucher: Don't overlook the fact that threats are categorized and that we examine them based on their type. That gives us information on the measures or methods that these businesses normally use. The measures we take are based on the threat type.

Mr. Michel Picard: Here's the challenge we're currently facing.

The CSE normally focuses on foreign, not Canadian, sources. In signals intelligence, however, signals have no citizenship. We don't know who's sitting at the keyboard. It may be a Canadian or a non-Canadian.

How can we tell the difference? How can we identify the threat to ensure, on the one hand, that these are indeed foreign signals and, on the other, that we have authority to act, since action has to be taken at some point.

[*English*]

Mr. Dan Rogers: You're absolutely right. CSE by mandate and by law can't direct its activities towards anywhere or anyone in Canada. Our foreign signals intelligence program is very much directed at foreign communications.

I can't get into the specifics of the way we do that, but I can say that where we do collect information, it's in accordance with the Government of Canada's set priorities. For us, that means we start from a foreign end for any intelligence activities, and from that foreign end we develop our intelligence products. We start from places where we are able to identify a foreign nexus to something, and then we evaluate from there. We never start from a Canadian or unknown end that is not clearly tied to a Government of Canada intelligence priority or to a foreign organization or individual.

● (1205)

Mr. Michel Picard: When you are an entity that tries to target our democracy—a process in general, such as a voting system—you either attack a person so that person will lose because his or her policies go against your interests, or you support a person, who will have to pay something in return because there's no free ride here.

Once you identify the attack itself, do you go further, asking what is behind the scenes of the whole thing, to see what justified this kind of attack?

Mr. Dan Rogers: Yes. We produce intelligence on exactly what the government requests. In the act, that is defined as the capabilities, intentions...I don't want to get the words wrong, but we look at the capabilities, activities and motivations of foreign states. That's included in the part of foreign intelligence. We seek to find as much rich information as we can about that, to provide to the government or other partners who can take action to respond.

Mr. Michel Picard: Is CSIS involved in that?

Mr. Dan Rogers: Certainly, we work with CSIS. We work with Global Affairs Canada, the RCMP and other domestic partners. Within their mandates, they'll use our information.

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

We move to the first five minutes, with Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Mr. Chair, my first question is for the Communications Security Establishment, the CSE.

A lot of digital information can now be posted on various platforms during an election campaign that lasts 35 to 40 days. In the event of an attack, how fast can you react in order to terminate it? If Elections Canada takes two or three days to notice an attack before issuing a report, the damage will continue in the meantime.

What can you say to reassure me on that point?

Mr. André Boucher: That's an excellent question.

In actual fact, the CSE already protects the Canadian government. Over the years, we've had to learn to deal with that kind of threat. You're entirely right. If it took us two days to react, we'd be in a very bad way. Consequently, we've put systems in place that can detect and follow a threat at its speed, what we, in our jargon, call working "at cyber speed".

That's exactly what happens with Elections Canada, an agency that we've been working with since 2015. We help it secure its networks and we put the necessary tools, systems and relational processes in place so that the time it takes to react to a threat is measured in minutes, not hours or days.

Mr. Jacques Gourde: You talked about Elections Canada's system, but I'm more interested in the misinformation circulating on certain platforms.

People can deny misinformation, but that takes time, and the harm is already done, not to mention the fact that the denial often reaches only a very small percentage of the audience that heard the misinformation in the first place. We've seen a lot of this in the United States, where information is determined to be fake news three or four days after it has spread. Can we guard against this kind of situation, or will we now have to live with it?

Mr. André Boucher: The cybersecurity responsibilities we have under our mandate limit what we can do to help you. The best thing we can do is help prevent the problems and ensure that people don't wind up in trouble.

You raise a very valid argument. However, once the threat he has emerged, the Canadian Centre for Cybersecurity unfortunately can't do much about it.

Mr. Jacques Gourde: What would be our limits as legislators if we wanted to amend certain telecommunications-related statutes in an attempt to improve the situation? Our authority is limited to Canada, and our laws don't apply if we're attacked from abroad. So it seems we're limited in that respect.

Mr. André Boucher: I'm not a legal expert, but I can tell you from experience that we've successfully combined individual and systems protections under our present laws to defend the Canadian government very effectively. I hope that evidence reassures you.

● (1210)

Mr. Jacques Gourde: Do you think Canadians can confidently anticipate that democracy will be respected in the next election campaign in view of the situation we have had in the past four or five years?

Mr. André Boucher: I'm extremely confident, and I'm convinced Canadians should be confident as well. This is the message I give my own children: go vote with confidence because a lot's been done over many years to guarantee our democratic process is sound.

Mr. Jacques Gourde: Thank you.

[*English*]

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

The next five minutes go to Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much. My first question is for Mr. Rogers and Mr. Boucher, and it goes back to the idea of who is being targeted.

Mr. Rogers, I believe you mentioned that it's more the politicians than the elections themselves who are the targets. Do you also find that female candidates and politicians are being targeted more?

Mr. Dan Rogers: I can't say that in my experience I know that to be true or false.

I don't know, André, whether you have a sense of that.

[*Translation*]

Mr. André Boucher: In fact, the study doesn't go into that level of detail. When we looked at the problem as a whole, we realized we could do something with Elections Canada and the machinery to protect the democratic process. However, where it was worth investing was in the politicians, the political parties and the media, all wide-ranging sectors.

[*English*]

Ms. Anita Vandenbeld: Anecdotally, we've heard a lot of evidence that women and female candidates are targeted, more particularly through the social media platforms. Some gender disaggregated data might be useful to the committee at some point.

Mr. Dan Rogers: Okay.

Ms. Anita Vandenbeld: Mr. Santor, this has to do with our ability to regulate our currency, because data itself is becoming a currency. We've seen the exchanges: You get a free coffee if you give us your email address. Then, of course, the data amalgamators are buying and selling this data on a large scale.

We saw in our study of Cambridge Analytica and SCL that, in some of the data that was found online, they were starting to work on a Midas token, a cyber currency.

What is the threat? If we start looking at data as global currency, and being paid for potentially through one of these cyber currencies, does this undermine our ability to regulate our monetary system?

Mr. Eric Santor: No, I don't think it does. It's a very interesting question that I'm certain we'll need to be looking at as digitalization proceeds in many different dimensions. But we have full faith and confidence in our currency.

Ms. Anita Vandenbeld: That's very good to know.

I'd also like to go to the competition issue. As legislators, our purpose is to legislate. With regard to the Competition Act, Mr. Santor, you had said that our competition policy doesn't need to be modified, that it just needs to have some additional tools; although I think heard, Mr. Durocher, you had made some indication that we do need to have some sort of changes in our Competition Act. Did I understand that correctly?

Mr. Anthony Durocher: I think in my opening statement I referred to following our study on the matter, we determined that the current framework was up to the task.

What really matters is the tools we use. I will preface my answer by saying that the Competition Bureau does not have the mandate to review competition policy. Our job is the enforcement side, and Innovation, Science and Economic Development now has the competition policy function. But certainly, our foremost priority is to make sure that we have the tools to handle the digital economy and we're seeing new issues come up. That's our focus and that's why we're very much prioritizing, consulting and staying on top of developments nationally and internationally.

Ms. Anita Vandenbeld: We've heard of a lot of these social media platforms like Facebook being called data-opolies—I think Mr. Santor said “superstar platforms”. The fact is that people don't really have a choice. If they're on Facebook, and all their data is on Facebook—their photos, all their family, all their connections, their networks—to go off Facebook and go to another platform, as long as that data is kept by Facebook, it's very difficult for people because it's become a very important part of our social norm. They essentially have become monopolies.

My question is whether or not the current tools that we have in the legislation are sufficient to be able to deal with that new kind of monopoly, which is these large data platforms.

● (1215)

Mr. Anthony Durocher: Canada's current competition framework is not meant to penalize monopolies per se. The competitive process ensures that firms that are innovating and investing and giving consumers a desirable product should not be punished for that. Our job is to ensure that these markets remain contestable through competition on the merits, and that small or existing or nascent firms are afforded the opportunity to compete on the merits of their products and services that they're providing to users.

Certainly, we're mindful of what's going on internationally on this front too, and we did note the GDPR has a data portability provision in it, which is noteworthy from a competition perspective as well. Our focus remains on ensuring that we have the cutting-edge tools to work with this. In our very broad consultation with our data paper, we consulted with the business, legal and academic communities.

There are no answers to this. There is no silver bullet. But we are confident that we have the tools to deal with it. We're going to keep them up to date.

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

The next five minutes will be shared by Mr. Van Kesteren and Mr. Gourde, but Mr. Van Kesteren is first.

Mr. Dave Van Kesteren (Chatham-Kent—Leamington, CPC): Thank you, Mr. Chair.

Thank you all for being here.

I'm not normally a member of this committee, but I did serve on this committee, as a matter of fact, when I was first elected 12 years ago, so it's kind of a homecoming for me.

I think the assumption of most Canadians would be that the Communications Security Establishment is well trusted. We believe in our Canadian institutions, and I would go along with that. I think you're doing a great job.

I'm curious. How many people work for your agency?

Mr. Dan Rogers: I think at this point it's somewhere around the order of 2,500.

Mr. Dave Van Kesteren: How many?

Mr. Dan Rogers: Twenty-five hundred.

Mr. Dave Van Kesteren: There are 2,500. That's a pretty good number, but when one looks at the NSA, for instance, in the United States and looks at.... First of all, there's just the enormity of their buildings. They have thousands upon thousands and thousands.

As I said in my opening remarks, most people would trust your organization, but what assurances do we have that organizations like the NSA...?

Mark Zuckerberg was in front of Congress a short number of months ago, and there were some real charges laid before that. There was collaboration between that organization, the CIA and a number of others. How do we not know that all of our information, all of the work that we do on all our files, isn't just being shifted about there?

Mr. Dan Rogers: Thanks for the interesting question and for your remarks about CSE being trusted.

In our context, we've had a very close relationship with our Five Eyes partners and our international allies in that space for a very long time, 70 years. The reason for that alliance is a shared set of values around things like protecting democratic institutions and a trusted alliance between our countries. We have conventions in the intelligence context that we don't target each other's citizens and a long history with them of ensuring that we have privacy protection measures that are afforded to each other's citizens as well as to our own. In the intelligence space, that's a long-standing practice and it continues today.

Mr. Dave Van Kesteren: I chose the United States, which is the largest group, I think, that would have the capabilities of doing whatever, but, of course, the Chinese are not far behind, and we've recently heard some disturbing reports of.... Somebody help me.

Ms. Irene Mathyssen: Huawei.

Mr. Dave Van Kesteren: Huawei. Those are, I think, more the issues that Canadians are somewhat concerned about. I know I certainly am.

What do we have in our defence mechanism to guard us from that type of foreign attack?

Mr. André Boucher: This goes to the security end of our organization.

Maybe piling on a little bit on what Dan has said about the team and the size of the team, the power of 2,500 is really the power of 2,500 plus our Five Eyes colleagues, and that helps you scale, when you're facing foreign threats of different kinds, of all kinds. We work very closely together. We share advice and guidance, and we share the perspectives on what the threats are, the methods that they use, and what to do about it.

On the specifics of countries or technologies, of course there will be moments when, within the Five Eyes, we might have different views and different opinions, but that's to be expected, because we're from different nations. We have different sovereign rights and different organizations, and we have different systems, in fact, and a different presence already. Where you see perhaps some discussions between us, our situation is different. We take different measures, but at the end of the day, around the table, when we sit down and look at a similar scenario, we always come to the same conclusion. Where there might be some differences on the surface, I assure you that, where it matters at the deep end, we are very closely aligned, and we have been for 70 years.

● (1220)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Mr. Gourde, you have 30 seconds.

[*Translation*]

Mr. Jacques Gourde: I'll be brief.

The security of confidential information is very important in Canada. For example, your cell phone numbers and email addresses will remain confidential if you don't give them out.

Two years ago, I was in Florida, where they have a public directory. I went onto the platform and typed in my name and address because I wanted to know whether a telephone number would appear. All my cell phone numbers and email addresses appeared on the screen. We can't do that in Canada. Canadians' personal information is secure and confidential, but it isn't in other countries.

Is there something we can do to correct that?

Mr. André Boucher: In the example you cited, it's a bit like the old white and yellow pages in the phone books that used to be distributed. There are varying degrees of information. If your information has appeared on the Internet, then it's all around the world because it's on several global servers. If you did the same search in Canada, you'd probably have found the same thing.

What's private is the information that's on your device and that you haven't shared. This goes back to previous questions. You have to be very careful when you share information. You have to read user contracts carefully and understand what you're committing to because you're dealing with a public network.

[*English*]

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

The next five minutes will go to Mr. Baylis.

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

Mr. Durocher, you said you did an investigation into Google. What did you investigate? You said they made a commitment to stop doing something. What did they commit to stop doing?

Mr. Anthony Durocher: Basically, the investigation was focused on search advertising and display advertising. Overall, we looked at seven potential theories of any competitive harm as to how competition may be hindered or how Google's actions were raising rivals' costs. On the balance of the evidence, we concluded that only one of those theories warranted taking action, and it essentially had to do with what's called the AdWords API terms and conditions.

It's a rather technical issue, but advertisers in the digital economy sometimes have to manage campaigns across different platforms, and essentially the inclusion of certain terms in that prevented advertisers from doing so effectively and using Google's rivals. This was dealt with with a five-year commitment that was provided to not introduce these terms and conditions into Canada.

I should point out that the Federal Trade Commission, which is our sister agency in the United States, had previously done a review and found the same issue as well.

Mr. Frank Baylis: My concern is that, as was already mentioned, the European Union and its commissioner who takes care of anti-competition, Margrethe Vestager, fined Google $3.6 billion. She said, “Google abused its market dominance as a search engine by promoting its own comparison shopping service in its search results, and demoting those of competitors.”

First of all, this sounds like anti-competition activity by our rules too. Did you investigate this?

Mr. Anthony Durocher: That's an excellent question.

That's why it's important to recognize that the competitive dynamics are not the same across countries necessarily. The European Commission has two decisions relating to Google. The one you mentioned is related to Google Shopping. Google Shopping did not figure prominently in our review, because the nature of the service that was introduced in Canada was really.... It came out in 2016. The introduction of these services are not the same across countries. That's why when we explore what other agencies are doing, we have to recognize that the nature of the services offered and the competitive dynamics are not necessarily the same as in Canada.

● (1225)

Mr. Frank Baylis: What Google was doing in Europe, you're saying, they were not doing in Canada, or did we not have laws to stop them from doing it in Canada?

Mr. Anthony Durocher: I would say the evidence suggested it did not raise an issue under our laws.

Mr. Frank Baylis: That means they could be doing the exact same thing in Europe as they're doing here, but in Europe it's bad enough that they get fined $3.6 billion, and here we say that it's not affected by our law. Is that what I understand?

Mr. Anthony Durocher: We're an evidence-based agency, and I would suggest that the evidence, as it pertains to countries in Europe, is not the same that we would consider here, nor the commercial realities—

Mr. Frank Baylis: Laws are structured such that the exact same thing could be happening in Europe and here, but here it's no problem, and there, it's a $3.6-billion fine.

Mr. Anthony Durocher: I would say not necessarily. If there were evidence that what Google was doing here was falling offside of our abuse of dominance provision, I can assure you we would take action.

Mr. Frank Baylis: But I want to talk about our abuses there.

Mr. Anthony Durocher: Yes.

Mr. Frank Baylis: Very specifically, if what happened in Europe was done here, would they be offside and get a big fine like that? Yes or no; it's a simple question.

Mr. Anthony Durocher: I can't hypothesize as to what they did in Europe and whether the same could apply here, because it's—

Mr. Frank Baylis: It's okay, if you haven't looked at it—

Mr. Anthony Durocher: We're driven by the evidence.

Mr. Frank Baylis: How many anti-competition fines are in the order of $3.6 billion? There can't be dozens of them such that you can't look into it. Your bureau hasn't taken the time to look to see what they're doing there, and whether they're doing the same thing here. It's a global company; it's a global search engine.

We'll hold that thought.

I think, Mr. Santor, you said the bank thought that our policies can be modernized. That was one of your statements. How so? What should we be looking at to modernize?

Mr. Eric Santor: That was a general statement, which is to say, as the economy evolves and as digitalization proceeds, it is not our responsibility, but that as new types of competition come up, using new technologies, it would be reasonable to expect that we would need to consider how to best modernize our practices in order to—

Mr. Frank Baylis: If you believe it should be, what should we do?

Mr. Eric Santor: That would be the responsibility of the Competition Bureau and the legislation to determine. What I was saying was that as the economy evolves, we'll need to evolve all our practices as well, to understand how competition is being affected by big data, because this is something that is new.

Mr. Frank Baylis: My concern here is that I see something of this magnitude going on. That's just one of the things I've heard. Other people have made major complaints about them using their search engine to direct users in one direction that financially benefits them and financially hurts their competition. I've read about someone who developed a much better search engine which they effectively killed. They've done a lot of this activity.

I cannot believe that it's only been happening in Europe, or if it is only happening in Europe—and I don't believe it— I'm concerned that our laws are not allowing you to do your job. That's what I'm trying to ask, Mr. Durocher.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Unfortunately, we're well past the five-minute mark.

Thank you, Mr. Baylis.

The last three minutes go to Ms. Mathyssen.

Ms. Irene Mathyssen: Thank you.

I guess the logical thing to ask is: Do our laws allow you to do your job?

Mr. Anthony Durocher: I think it's important to say yes. Canadians can take comfort that we are taking all steps necessary to vigorously investigate and take action when warranted. The underlying premise needs to be that we make principled, evidence-based decisions. We cannot have theory dictate our actions under the Competition Act. I would suggest to this committee that that is a very important takeaway.

Were any of these digital giants engaging in conduct that is meant to harm competitors, that could very well raise issues under the Competition Act, and these are the types of issues we would investigate, but the evidence needs to bring us there.

Ms. Irene Mathyssen: Thank you. I think, in regard to Huawei, that was part of what we heard, that they were indeed harming Canadian companies. In the case of Huawei, it was Nortel, which is gone now.

Do you think that with built-in encryption, the back doors risk the bad actors permanently compromising encryption?

● (1230)

Mr. Dan Rogers: Sorry, just to clarify, could you expand on back doors?

Ms. Irene Mathyssen: Are the bad actors able to access built-in encryption systems?

Mr. Dan Rogers: I can say—André please jump in if you'd like—when we observe things in foreign intelligence space, we do find nation-states and other actors making use of vulnerabilities in software in order to defeat things, like encryption, and to gain access to communications that should otherwise be protected.

When we see this in a foreign space, we will provide information of that type to our colleagues in the cyber centre and other agencies in Canada that take action, which might include providing mitigation advice or notifying vendors to make sure that those back doors are dealt with.

Ms. Irene Mathyssen: In the description about the Russian penetration of the American election system and the Netherlands, it was indicated that these were low-level characters. This was not a sophisticated bunch doing this.

What happens when a more sophisticated bunch comes along? You talked about best practices and what you called a hygiene guide. I wonder if you could explain who is using that guide, and how it is effective. Can we count on it, based on the fact that human beings are involved? Should we take comfort from the hygiene guide?

Mr. André Boucher: Absolutely. Part of the challenge for the Canadian Centre for Cyber Security is developing advice and guidance for all people operating in the cyber environment. One key element of the cyber environment, for you and I and users of that environment, is the cyber hygiene guide, advice on how to use mobility. There is a body of knowledge you can find on our website. It also gets shared through cyber-safe campaigns and other campaigns. That is specifically targeting simple measures that everyone can take that give the most benefit for a few actions.

When we write the advice and guidance, we do it in the spirit of getting the most benefit in security terms with a few simple actions.

Ms. Irene Mathyssen: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): I have a few questions.

I want to start with you, Mr. Rogers, and it's a really simple question.

Political parties get their backs up when we talk about potentially bringing them under a regulatory framework with respect to privacy or data protection practices. I'm glad you've given advice to all Canadian political parties.

My question is not so much from a privacy protection standpoint, but from ensuring best data management practices. I attended a parliamentary round table of representatives in Washington. Bob Zimmer was there as well. A number of representatives say that two-factor authentication is necessary in today's day and age, and if it's not a rule for political parties, that's a huge problem.

I read your June 2017 report, and you say you're not worried about Elections Canada, but you're worried about the vulnerability of political parties. When I read that the Democratic Party and the Republican Party were both hacked and that there was selective distribution of the material from that hacking, it's political parties that need to up their game on data management practices.

Shouldn't they be regulated?

Mr. Dan Rogers: I don't think it's for us to say what the Canadian government's regulations should be. André could speak to the types of things we would suggest that anyone, political parties and others, would take on board if they want good cyber hygiene practices.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): To put it a different way, do you think it would be better for the protection of our information or for the security of our elections if your advice became a rule?

Mr. André Boucher: If I may jump in, based on years of practice, I'll share with you my position on rules.

We work in collaboration, as I mentioned, with all participants. People want to secure themselves. All entities and political parties genuinely want to do that.

When I work on a model of collaboration and best practices, I reach a certain threshold of delivery and outcome. The minute I establish a standard—and there are many standards in production of equipment, tables, chairs and what have you—there's a race to the bottom. People try to meet the minimum standard because there's competition at play. Best practices are done through collaboration.

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

Mr. Durocher, in your report, the white paper, it indicates that the purpose of the act and the review, when you look at big data, the goal really is to ensure an innovative, efficient and prosperous economy. There's a conversation about substitutability. It's not just the price; you could talk about quality.

We had some folks here talking about the worries about antitrust. It was on this point, quite apart from pricing. People are put in a position—Ms. Vandenbeld got at this—where you're forced to deal with a monopoly.

We have the Bank of Canada suggesting that the five biggest global tech companies have a market cap of $3.5 trillion U.S. There are certain companies we have to deal with in our day-to-day lives. There's no choice to be made. We have to give up what we give up to access the service. It's not necessarily a price consideration, but there's a quality consideration. Part of that quality of service is the data and the privacy that I potentially give up.

That was not a big part of the conversation when you were looking at big data in the paper. I wonder if you could speak to that.

● (1235)

Mr. Anthony Durocher: Sure. That's a great question, great observations, and I can tell you that when Professor Maurice Stucke appeared before this committee, we reviewed the transcript with great interest, because we are following what thought leaders such as him have to say on the matter.

I completely agree that in the digital economy, we've moved from what we call static competition to dynamic competition. Static competition is this old-world competition on price and output which is still prominent in a lot of industries across Canada. In the digital space, what we're seeing is that companies largely compete for users on the basis of how they're innovating in the offer of their products to consumers. We call this non-price effects. When I talk about modernizing the tools we use for the Competition Act, it's exactly with a view to addressing these issues of non-price effect.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Great.

Another thing talked about in your white paper was a barrier to switching services. It's not so easy for me to print out everything from Facebook and move it over to another network. It occurs to me that another barrier is network effects, but as your paper indicates, there are great positive benefits that come from network effects.

I don't know what the positive benefit is from the barrier to switching. I know that when you look at the GDPR and you see a rule about the right to portability, and others have talked about not just a right to portability but a right to interoperability as well, wouldn't that increase competition?

Mr. Anthony Durocher: Yes. That's an excellent question as well.

Data portability of the regulations that we're seeing through the GDPR is the most noteworthy, I think, from a competition perspective. In theory, it can be pro-competitive. It can empower consumers to take their data from one platform to another. Obviously the devil is in the details as to how that's operationalized, but certainly it's something we're taking note of.

We're seeing it in the Canadian banking industry. For instance, the underlying premise of the open banking initiative is enabling people to move their data from one service provider to another. From a competitive perspective it's certainly very interesting. It's something we're monitoring very closely.

By the same token, we have to watch how it's operationalized. From a competitive perspective, when we look at regulations relating to privacy, another competition consideration involves the cost of compliance. It must not be so high as to effectively entrench large players and make it more difficult for smaller players to compete.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Don't you think that when you look at those other factors beyond price and privacy, which is something that this committee has obviously been concerned with, the notion of privacy by default would level the playing field? Wouldn't it take away that unequal bargaining power between the monopolies, as it were, and the individual consumer? An individual wouldn't have to immediately give away all of his or her privacy rights right from the get-go. We'd get at some of those other factors related to substitutability beyond price.

Do you think that would be a useful conversation for us to have?

Mr. Anthony Durocher: It certainly could be. We would advocate that market forces should drive improvements in all dimensions, including privacy.

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

Mr. Santor, this is my last question.

Ms. Wilkins, senior deputy governor, remarked in February of this year that data has become another source of monopoly power. She indicated two concerns. One, it might impact innovation in a negative way, and two, it may well return to monopoly pricing in the long run.

There may be some other concerns. We've certainly heard some other potential antitrust concerns from other witnesses here.

She threw out some potential solutions that other people have been talking about regarding how we regulate ownership and the sharing of information, and maybe treating tech platforms as utilities.

When we had the CRTC here on net neutrality, they talked about a section that says companies can't unjustly discriminate or give undue reasonable preference towards themselves—or any person, but including towards themselves—or subject any person to unreasonable disadvantage. That's to get at equal treatment.

Should we regulate Facebook, Google, Apple, Amazon and Microsoft? Shouldn't we treat them the same as Rogers and Bell?

● (1240)

Mr. Eric Santor: That's a question beyond the mandate of—

The Vice-Chair (Mr. Nathaniel Erskine-Smith): She suggested treating them as similar to utilities, though.

Mr. Eric Santor: That question is best discussed by those who have the expertise to decide whether or not the competition.... To fully realize the benefits of digitalization, we need to ensure that competition is effective.

We need to be asking these questions, but it's an open question as to how best to do that. I would defer to my colleagues on that.

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

The only thing I would say is that I'm very glad Ms. Wilkins raised the concerns and identified the problem. If she happens to have any solutions she wants to offer, she's welcome to propose them.

Does anyone else have any questions?

We have Mr. Picard with a question, Mr. Baylis with a question, and then Ms. Mathyssen.

[*Translation*]

Mr. Michel Picard: Ms. Gendron-O'Donnell, you clearly indicated, in response to a question, that you should be able to ensure that what's stated in contracts is transparent.

To improve your investigations, are there any changes or things you would like to recommend to the committee? We talked about misuse and misleading information. Is omission part of that? Are there aspects of your regulations that should be amended to improve your ability to investigate?

Ms. Alexa Gendron-O'Donnell: Thank you for your question.

As my colleague told you, political issues or matters concerning the Competition Act do not come under the Competition Bureau's mandate. We are satisfied with the current provisions of the Competition Act, and the department handles those aspects. We do as much as we can with the resources at our disposal. We focus our efforts on areas where we can have the biggest possible impact, and we target investigations that will have the most positive impact on Canadians.

Mr. Michel Picard: My next question is for the CSE representatives.

In your understanding of a threat, do you draw a distinction between the enormous quantity of information that's dumped onto social media and that confuses people and direct attacks or piracy? Most readers no longer know what to think, how to think or what to look at. In fact, it's all outright propaganda.

Is there another aspect that would be similar to piracy but that falls under your responsibility and constitutes a threat? You have to draw distinctions among things. The government has to be able to take action on the right thing. It can't interfere with someone's right to say what he wants, even if it's nonsense. On the other hand, if people post things in places where they shouldn't, the government's entitled to act.

Do you distinguish between the two at your level?

[*English*]

Mr. Dan Rogers: I can speak to the foreign intelligence side of that question, and that is to say that regardless of the method, whether it's hacking or sending disinformation, whatever the technique of a foreign government is, for instance, or of an organization that would seek to do Canada harm, we would be interested in that so long as it is a government intelligence priority. From the foreign intelligence side, both of these things may be distinct, but we would be interested in either.

From a response point of view, André, did you want to comment on that?

[*Translation*]

Mr. André Boucher: Yes.

Mr. Picard, as you mentioned, we examine the threat and the method normally used. We focus on the confidentiality, integrity and availability of systems and networks. Information conveyed over those networks does not come under the CSE's responsibility. We ensure that information, whatever it may be, is safely saved, protected and transmitted.

Mr. Michel Picard: I see. Thank you.

[*English*]

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

Mr. Baylis, you have a few minutes. We want to finish up by 12:50 p.m., so we can go in camera and discuss some committee business.

Mr. Frank Baylis: Mr. Rogers, in your presentation, you're looking at cyber-threats to Canada's democratic process. We just had Aggregate IQ, a Canadian-based company, busily interfering with the U.K. Brexit vote and, we believe, also the American presidential vote which President Trump won.

They were using stolen data. It was Facebook's stolen data. Are they captured in what you investigate? Or are you only outward-looking? If they're sitting here in Canada and they're interfering with other people, we'd be foolish to believe that tomorrow they're not going to turn around and interfere with their own. Are there limits on what you can investigate? I'm quite bothered that we have a Canadian entity actively interfering and thumbing their nose at our committee as they do it.

● (1245)

Mr. Dan Rogers: It is part of our lawful mandate to look only at foreign threats outside of Canada. A Canadian company engaging in any type of behaviour would not be within our mandate in the foreign intelligence side to investigate, but there may be other entities in Canada where that would be within the mandate. I can't speak to that, but CSIS, RCMP and others have more of a domestic focus than we do.

Mr. Frank Baylis: If I understand it, you're the chief of foreign signals intelligence. Is that the catchword for cybersecurity?

Mr. Dan Rogers: That's our foreign intelligence collection apparatus within CSE. André is the assistant deputy minister for operations on the cyber side. That's the centre that will respond to cyber-threats and advise. We do the intelligence collection that might inform their activities and other activities in government.

Mr. Frank Baylis: Do you interface with other foreign entities that are also looking at getting hacked themselves? Did the Americans or the British people contact you to coordinate specifically with respect to what AIQ is up to?

Mr. André Boucher: The Canadian Centre for Cyber Security is in fact one of many such national centres. We work very closely with similar centres and the Five Eyes, but also with centres around the world. Part of the centre also is the national CERT, the national element that does emergency response teams, which is part of a global network. You have layers of cybersecurity practitioners working together and sharing—where they can—information that's relevant for their mandates.

Mr. Frank Baylis: Who in Canada should be dealing with AIQ and what they've been up to?

Mr. André Boucher: On the basis of what you said, which was on the basis of stolen information, this would be an RCMP mandate.

Mr. Frank Baylis: What they've claimed is that they built the software and they never touched the data. That's an actual argument. They've said that they never had access. They didn't touch the data, they said, or they had small pools of data. They were careful to massage around it, but clearly they built the programs or software. They used the data to actively interfere. They did break certain other rules in the U.K. We know about that.

Does the RCMP have the cybersecurity to look at it from a stolen data perspective? What about looking at it simply in terms of interfering with the democratic process? There are two separate things. One thing is that, okay, they stole something, and the other thing is what they're doing with what was stolen.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Please respond briefly and we'll leave a couple of minutes for Ms. Mathyssen as well

Mr. André Boucher: Very briefly, when the cyber centre receives a call from a victim on information stolen, identity stolen, we direct that call to the RCMP and they have the authority and the mandate to take action.

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

Ms. Mathyssen, you have a couple of minutes.

Ms. Irene Mathyssen: Thank you very much, Mr. Chair.

Again, thank you for all of this information.

I did have a question in regard to the tech giants. Most of them are American and they wield substantial influence beyond the U.S. border. We know that. Should the monopoly power of these tech giants be addressed in international trade agreements in which the U. S. or any parent country is participant, and if so, how would you go about it?

Mr. Anthony Durocher: I'm happy to answer that.

Ultimately, in competition law we deal with transborder companies all the time. We review conglomerate mergers. Certainly in the tech space, a lot of decision-making and relevant information is outside of Canadian borders. Critical for us is to have access to that and to have jurisdiction over that.

With respect to trade agreements, I think that's beyond our mandate. I'm not well placed to opine on that. What I can tell you is we have excellent relationships with our foreign counterparts who enforce their respective antitrust laws and we're constantly communicating with one another.

Ms. Irene Mathyssen: You may not be able to answer this, but I wonder if there should be things built into these trade agreements. The reality is that parliamentarians, and by extension, the citizens whom we serve, don't have access to the texts of trade agreements until after the government has ratified them. Should there be greater transparency? Do we need to know more?

● (1250)

Mr. Anthony Durocher: The Competition Bureau has an international group that participates in trade agreements, and a lot of trade agreements have competition chapters. The new USMCA has a competition chapter in it that is largely geared towards ensuring the sound exchange of information between agencies to enable them to work collaboratively and to do their jobs, because as I said, a lot of antitrust is international in scope. You have international cartels, conglomerate mergers that are notifiable in dozens and dozens of countries, and business conduct that can be international in scope as well.

Really, our job is to make sure that we maintain those relationships and that we're communicating with one another, given how international the activity is.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Unfortunately, we're out of time, but thank you to all of our witnesses here. If you do have additional thoughts that you want to share with the committee on this subject, please submit them in writing.

With that, we'll suspend for a couple of minutes to clear the room, and we'll come back in camera to deal with some committee business.

[*Proceedings continue in camera*]