HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 134 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 5, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 5, 2019

● (1545)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Welcome, everybody, to the Standing Committee on Access to Information, Privacy and Ethics, and meeting number 134, on the privacy of digital government services.

We have with us today, as individuals, David Carroll, associate professor, Parsons School of Design, The New School; Chris Vickery, director of cyber risk research, UpGuard; and, from Digital Content Next, Jason Kint, chief executive officer.

Before we get to you guys—again, our apologies for voting, which is why we're here a little late—we have a motion that was discussed on Thursday that we're going to bring forward.

Mr. Kent, go ahead.

Hon. Peter Kent (Thornhill, CPC): Thank you very much, Chair. I think we can deal with this quite quickly.

Since our last meeting, there have been discussions with the Liberal vice-chair, and I've been informed that the new committee is so new that it hasn't yet had an opportunity to meet.

I'll refrain from suggesting that the government seems to have announced it on the fly, but I would like to amend my motion from Thursday to replace “senior officials”, so that it would read: “That the Committee invite the Minister to appear on behalf of the newly formed Security and Intelligence Threats to Elections Task Force to discuss the vision, the challenge and operating protocols.”

The Chair: Is there any discussion on the changes to the motion?

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): No. I think that's a reasonable amendment, and I think Minister Gould is best placed to answer the questions we have at this time.

Hon. Peter Kent: What a reflection of our collegiality.

Mr. Nathaniel Erskine-Smith: Indeed.

Mr. Raj Saini (Kitchener Centre, Lib.): Wow, that's a bit cheeky.

Mr. Nathaniel Erskine-Smith: It's only because I like you, Peter.

The Chair: Mr. Cullen.

Mr. Nathan Cullen (Skeena—Bulkley Valley, NDP): The only thing I would not necessarily add but say just for the committee's own perspective is that we've had conversations with Elections Canada about this procedure as well. I think the committee should be open to talking to the head of Elections Canada as well, who is of course an officer of Parliament and whose sole and single mandate is to ensure that free and fair elections happen in Canada, which is also the purview of this committee with respect to this one aspect of foreign interference and fake news. I don't know; I didn't ask this of the CEO, but I suspect the the CEO might have some things to contribute to that kind of conversation.

Hon. Peter Kent: So we have an amendment to the subamendment?

Mr. Nathan Cullen: I wasn't even proposing it as an amendment

Hon. Peter Kent: Could it be an eventual...?

Mr. Nathan Cullen: Yes. Just be open to it and aware that this is somebody who obviously knows a great deal about elections and is in charge of running the next one.

The Chair: I'm just getting word that you would have to get Mr. Gourde to amend your own motion.

Hon. Peter Kent: Monsieur Gourde?

The Chair: Mr. Gourde said he would amend it per the above. That's good.

Is there any further discussion?

(Amendment agreed to)

The Chair: All in favour of the motion?

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): As amended.

The Chair: As amended, thank you.

(Motion as amended agreed to)

The Chair: Thanks, everybody.

We'll get going.

Mr. Carroll, would you start, please? You have 10 minutes.

Mr. David Carroll (Associate Professor, Parsons School of Design, The New School, As an Individual): Thank you to the chair, the vice-chair, and the committee members for the opportunity to give evidence today. I have followed the work of this committee as it relates to Cambridge Analytica fairly closely, especially as it has intersected with investigations in the United Kingdom and the United States. I have been impressed with the committee's unwavering efforts to fact-find and truth-tell as it has probed the company entangled in the transnational election and data crimes investigations of 2016: AggregateIQ, an exclusive vendor of SCL Elections Limited, which is the registered data controller of Cambridge Analytica in the United Kingdom.

Kindly allow me to offer a brief chronology of my personal effort to win full disclosure of an SCL Elections voter profile generated from the 2016 presidential election cycle, under the U.K. Data Protection Act of 1998, in the courts and through enforcement actions of the U.K. Information Commissioner's Office.

In January 2017, I filed a subject access request at cambridgeanalytica.org to request my voter file, after being advised this was possible. I was instructed to pay SCL Elections Limited a £10 fee and provide copies of government ID and a utility bill to validate residency.

In March 2017, I received an attempt from datacompliance@sclgroup.cc to be compliant with the U.K. Data Protection Act of 1998, which included a letter signed by SCL Group chief operating officer Julian Wheatland, and an Excel spreadsheet with voter registration data and an ideological model consisting of 10 political topics ranked with partisanship and participation predictions. I expected to receive much more data, as Alexander Nix, Cambridge Analytica's CEO, had frequently boasted of collecting up to 5,000 data points for each U.S. voter.

In July 2017, I filed a complaint with the Information Commissioner's Office under section 7 of the U.K. Data Protection Act that SCL Elections Limited had refused to answer any questions or respond to any concerns regarding the data provided.

In October 2017, I launched a crowdfunding campaign to file a claim in the High Court of Justice against SCL Elections and related companies.

In February 2018, I gave evidence to the U.K. House of Commons select committee on digital, culture, media and sport when it convened hearings in Washington, D.C.

In March 2018, I filed and served SCL Group and Cambridge Analytica with a section 7 Data Protection Act claim demanding full disclosure of my voter profile providing expert witness statements that evaluated how the provided data could not possibly be complete.

In May 2018, the Information Commissioner's Office issued an enforcement notice to SCL Elections Limited, to comply with its order to fully disclose my voter data file, under criminal penalty.

In June 2018, while giving evidence to the LIBE committee in the European Parliament, on the dais with the information commissioner and deputy information commissioners present, SCL Elections failed to respond to the enforcement order as the deadline expired, as we were sitting there in Brussels.

In December 2018, I instructed an insolvency barrister to challenge the administrators attempting to liquidate most of the SCL Group companies, and I won a court order to get disclosure of the complete administrators' filings, which they refused to share with us.

In January 2019, the ICO prosecuted SCL Elections for failing to respond to its enforcement order to disclose my data. Despite publishing an intent to plead not guilty in its public filings, the joint administrators entered a surprise plea of guilty, then paying court fines and costs. It was reported at this trial that the ICO finally received passwords to servers seized from Cambridge Analytica/SCL under criminal warrant in March 2018. According to court-ordered disclosures I obtained in December 2018, the ICO was seeking these passwords potentially as early as May 2018.

● (1550)

In March 2019, the high court in the U.K. will hear our challenge to the joint administrator's proposal to liquidate the SCL Group companies. Evidence will be presented that highlights concerns that the administrators and directors have misled the court on critical matters. In addition, the high court is notified of evidence discovered by Chris Vickery, another panellist today, that indicated how former Cambridge Analytica and SCL employees had been building new companies while accessing databases of CA/SCL that remain in the cloud.

We will continue to pursue complete disclosure of my data file and won't give up until fully vindicated. Both the ICO and the DCMS committee have repeatedly expressed the clear understanding that because U.S. voter data was processed in the U.K. by SCL, the Data Protection Act applies and the ICO has jurisdiction.

The quest to repatriate my voter file from the U.K. teaches us so much about the fundamental data rights that the United States and Canada have not yet assigned and protected for their citizens. We can now clearly understand how the right of access underpins the essence of data protection as a key to sustaining democracy in the 21st century.

We can also better understand how data protection and data privacy policy interconnects with other legal frameworks, such as international treaties, bankruptcy, insolvency law, election law, campaign finance, and even antitrust.

I look forward to being able to answer the committee's questions about my journey in reclaiming my Cambridge Analytica data and what it might portend for the future of our digital democracy.

Thank you.

● (1555)

The Chair: Thank you, Mr. Carroll.

Next up, we'll go to Mr. Vickery via teleconference, and then to Mr. Kint, afterwards.

Go ahead, Mr. Vickery.

Mr. Chris Vickery (Director of Cyber Risk Research, UpGuard, As an Individual): Hello. It is a pleasure to appear once again before the committee. I've always enjoyed speaking with you, and feel that I can bring a lot to the table.

I reviewed the previous meetings' recordings for this specific subcommittee, talking about data and privacy along the pathway of moving Canada to digital online government services, and where things are now and where they are going to be, as well as different concerns the committee has. While I am open to answering questions about the AggregateIQ/Cambridge Analytica situation, I will not focus on that in my opening remarks. I am going to address some issues that were brought up in those previous meetings that I listened to and reviewed just recently.

Right now, it feels that Canada needs to make a decision on which direction the tech strategy needs to go in, or wants to go in. There is an opportunity to jump headlong into the game with all of the other big players and to try to be on the leading edge of the government digital crossroads, but it seems to me that the most natural position from what I heard in the previous discussions is to take a stance of, okay, let the other guys make the mistakes and do the advance running, sprinting at the head of the crowd, and then incorporate the things that work into your systems, and not the things that don't work. That seems to be the most advantageous position that I heard.

Another contention was on whether or not it should be mandatory to bring people into this digital environment, whether Canadians feel wary or not or trusting enough to give all of their personal data, medical data, over to a Big Brother type of situation. If you make it mandatory, then when there is, or if there is, any sort of data breach or vulnerability or problem that's taken advantage of, you risk a huge hit in public confidence in the system.

I would recommend that Canada try to have it be adopted by success, rather than being forced upon people, so that if a neighbour, by word of mouth, tells somebody else, “I made an appointment with my doctor; it was so easy, you should get online and do this, too”, that would be a lot better than if there were a data breach and those two neighbours were then talking about how much they hated being forced into the situation.

I heard a lot of discussion about blockchain, and some people trying to float the opinion that blockchain is going to solve things. I would be very wary of blockchain technology in its current state, and even in the future. Blockchains are basically where everybody has everything. It's a distributed ledger. It's not necessarily a secret key thing, or technology. I believe the great many failures of various coins on blockchains have indicated the somewhat inevitable issues that can crop up, and it's just not mature enough to be handling medical data and personal data, and especially for voting. That's a nightmare.

Another issue that was brought up was anonymizing data, and how important it is to have these pools of data so they can be studied and shared among the government departments and easily ported from one database to another, and how great that can be. Yes, you can get some great insights from that sort of study and looking at everything from a meta, overall angle, but there really is no such thing as anonymized data. It's a little bit of a misnomer. You can have data that you redact certain elements from, or drop certain things and try to make it hard to re-identify the people, but all you actually do when you anonymize data is that you make it harder and harder for the little players to re-identify folks. I guarantee that the big data brokers and the banks and the insurance companies can re-identify the data in most anonymized datasets simply based upon what they have already and are able to reference. It's just a matter of how much data the entity has that determines how long it takes them to re-identify it, so be very careful with anonymized data and thinking it's foolproof.

I don't just want to bring up issues or problems. I also want to bring forward some ideas, some brainstorming, of different ways to implement secure data-sharing among various government departments. The idea that privacy and security is built in by design is very powerful.

● (1600)

I think there is an opportunity for you to take the mindset of asking, if you were creating all of existence and you could create the laws of physics, the fundamental building blocks of the ecosystem that your data is going to live in, how you would do it so that it's secure.

I would do it in a way that database A and database B don't even speak the same language, can't communicate with each other, cannot pool data together, and I'd have a translator in the middle that they pass the data to, which would then translate it to each other.

That's just an idea I had. The advantage there is that you can have the translator be not available 24 hours a day, seven days a week, so that when everybody is asleep on a Saturday night, you don't have to worry about a bad guy getting into one and being able to access all of the others. It's all about segmentation, breaking things into pieces, compartmentalizing. Even though that makes it a little bit harder on the programming end of things, I think you'll get a much better outcome if you plan this sort of thing ahead of time, do it the right way and make sure everybody involved is of the right mindset.

Finally, I want to say that if there's one thing that needs to be done the old-fashioned way, it's voting. Digital voting is laden with all sorts of problems, with corruption. If there's one thing we need to do with hand-marked papers, it is voting. I'm very disappointed in how the United States has come to handle voting, and I wish much better for your country.

Thank you.

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

We'll go to Mr. Kint, for 10 minutes.

Mr. Jason Kint (Chief Executive Officer, Digital Content Next): Good afternoon.

Thank you for the opportunity to speak before your committee today. I have closely followed the work of this committee, including its superb representation by the chair and vice-chairs in last November's International Grand Committee on Disinformation and 'fake news'. I am honoured to be here, and I appreciate your overall interest in consumer privacy.

I am the CEO of DCN. Our mission is to serve the unique and diverse needs of high-quality digital content. This includes small and large premium publishers both young and centuries old. To be clear, our members do not include any social media, search engine or ad tech companies. Although 80% of our members' digital revenues are derived from advertising, we are working with our members to grow and diversify.

DCN works as a strategic partner for its membership by advising and advocating with a particular eye on the future.

As you are aware, there are a wide variety of places where consumers can find online content. In light of this dynamic, premium publishers are highly dependent upon maintaining consumer trust. As an organization, DCN has prioritized shining a light on issues that erode trust in the marketplace, and I'm happy to do so today. This makes enhancing consumer privacy while also growing our members' interests a critical strategic issue for DCN.

Over the past decade, there has been a significant increase in the automation of content distribution and monetization, particularly with advertising. We've shifted to a world where the buying, the bidding, the transacting, and the selling of advertising happens with minimal human involvement. We do not expect nor do we seek to reverse this trend, but today I hope to explore with you a few of the major challenges impacting the industry, the public and democracy.

The first area I would like to explore is the rise of what your December report aptly labels "data-opolies". Unfortunately, an ecosystem has developed with very few legitimate constraints on the collection and use of consumer data. As a result, personal data is more highly valued than context, consumer expectations, copyright or event facts.

Today, consumer data is frequently collected by unknown third parties without any consumer knowledge or control. Data is then used to target users across the web, without any consideration of the context, and for as cheaply as possible.

In our mind, this is the original sin of the web—allowing for persistent tracking of consumers across multiple contexts. This dynamic creates incentives for bad actors and sometimes criminal actors, particularly on unmanaged platforms like social media where the bias is for a click, whether it's from a consumer or a bot.

What is the result? A massive concentration of who is benefiting from digital advertising, namely Google and Facebook. Three years ago, DCN did the original analysis, including giving them the label of "the duopoly". The numbers are startling. In the $150 billion-plus digital ad market across North America and the EU, 85% to 90% of the incremental growth and over 70% of the total ad spend is going to just these two companies.

Then we started digging deeper and, as in your report, we connected their revenue concentration to their data practices. These two companies are able to collect data in a way that no one else can. Data is the source of their power. Google has tracking tags in which they collect data on users across approximately 75% of the top one million websites. We also learned, thanks to evidence provided in the U.K. to the DCMS committee, that Facebook has tracking tags on over eight million sites. This means that both companies see much of your browsing and location history.

Although your work is mostly focused on Facebook, we would strongly encourage you to also review the role of Google in the digital ad marketplace. DCN recently helped distribute research conducted by Dr. Doug Schmidt of Vanderbilt University, which documented the vast data collection of Google.

Google has used its unrivalled dominance as a browser, operating system and search engine to become the single greatest beneficiary in the provision of ad tech services. Google has no peer at any stage of the ad supply chain, whether buying, selling, transacting or measuring advertising. In any other marketplace, this would be illegal. In the financial world, it is akin to being the stockbroker, the investment banker, the stock exchange and the stock itself.

Therefore, we believe that recommendations 12 and 13 in your report are important as you seek to understand the clear intersection between competition and data policy. The emergence of these data-opolies has created a misalignment between those who create the content and those who profit from it. It has also allowed a vicious cycle in which the industry rules and the consumer privacy bar are set to protect incumbent industry interests rather than consumer trust.

● (1605)

We would also encourage you to further explore law professor Maurice Stucke's arguments, along with Anthony Durocher's from your Competition Bureau, recommending a shift beyond price-centric analysis as companies offer free products to exploit consumer data. With the U.K. ICO's findings regarding Facebook's privacy practices from 2007 to 2014, which your own report labels as “severe”, I would call attention to a research paper published last week by Dina Srinivasan, titled “The Antitrust Case Against Facebook”, in which Ms. Srinivasan documents this bait and switch by Facebook in its early years, originally using privacy protection as a paramount differentiator in a very competitive set of free products of social networks that were forced to compete on quality and, over time, lowering the quality of privacy.

Finally, the scandal involving Facebook and Cambridge Analytica underscores 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 that data. Facebook's data was ultimately sold to Cambridge Analytica to target political ads and messaging, including in the 2016 U.S. elections.

With the power Facebook has over our information ecosystem, our lives and our democracy, it's vital to know whether or not we can trust the company. Many of its practices prior to reports of the Cambridge Analytica scandal clearly warrant significant distrust. Although there has been a well-documented and exhausting trail of apologies it's important to note there has been little to no change in the leadership or governance of the company. With this in mind, there is an acute need to have a deeper probe, only made more apparent by the company's repeated refusals to have its CEO offer evidence to DCMS and your grand committee. They've said the buck stops with CEO Mark Zuckerberg, but at the same time he's avoided the most difficult accountability questions. There is still much to learn about what happened and how much Facebook knew about the scandal before it became public. The timeline is troubling to me.

We learned from Mr. Zuckerberg's testimony to the U.S. Senate judiciary committee that a decision was made not to inform Facebook users that their data had been sold to Cambridge Analytica after *The Guardian* reported in December 2015. *The Guardian* reporter had said he reached out to GSR as early as late 2014, nearly a year before reporting on it. GSR co-founder Aleksandr Kogan testified to Senator John Thune that he and his partner had met with Facebook several times throughout 2015. Even more incredulous to me was that Facebook hired to its staff Kogan's so-called equal partner at GSR, Joseph Chancellor, on November 9, 2015, an entire month before *The Guardian* reported. Time and again, Facebook has been asked when exactly Mr. Zuckerberg became aware of Cambridge Analytica, yet Facebook only offers a non-answer by replying that he became aware in March of 2018 that the data had not been deleted. On a personal note, I find this answer offensively obtuse.

Considering that the FTC has a consent decree with Facebook to report any wrongful uses of data, it's incredibly relevant to know when its CEO was first aware of Cambridge Analytica. We now know Facebook spent significantly more time and resources in 2016 helping Cambridge Analytica buy and run ad campaigns than they did trying to clean up their self-titled “breach of trust”. Although Facebook's CEO testified to the U.S. Congress in April 2018 that they immediately worked to have the data deleted upon being made aware in 2015, Facebook has already submitted evidence to DCMS that no legal certifications happened with Cambridge Analytica until well into 2017 when its CEO returned a fairly useless piece of paper.

Finally, Facebook disclosed in September 2018 that Mr. Chancellor no longer worked at Facebook without any explanation after a nearly six- months-long investigation, which began only after the TV show *60 Minutes* drew further scrutiny to his role.

Equally troubling in all of this, other than verbal promises from Facebook, is that it's not clear what would prevent this from happening again. Moving forward, we urge policy-makers and industry to provide consumers with greater transparency and choice over data collection when using practices that go outside consumer expectations. Consumers expect website or app owners to collect information about them to ensure that the site or app works. Indeed, data collecting used within a single context tends to meet with consumers' expectations, because there is a direct relationship between these activities to the consumer experience, and because the consumer's data is collected and used transparently within the same context. However, as happened in the case of Facebook and Cambridge Analytica, data collected in one context and used in another context tends to run afoul of consumer expectations.

● (1610)

Also, it is important to note that secondary uses of data usually do not provide a direct benefit to consumers. We would recommend exploring whether service providers that are able to collect data across a high threshold of sites, apps and devices should even be allowed to use this data for secondary uses, without informed and specific consent. A higher bar here would solve many of the issues previously mentioned.

Finally, it is important to shed light on these practices and understand how best to constrain them going forward. I appreciate your efforts to better understand the digital landscape. By uncovering what happened and learning from it, you are helping to build a healthy marketplace and to restore consumer trust.

The Chair: Thank you, Mr. Kint.

We'll start with a seven-minute round of questions. First, we have Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much.

I'm going to go around with some different questions for each of you.

I appreciate your all being here today.

Mr. Vickery, I want to start with a question on digital government, which is the principal focus of the next few weeks of our time here at this committee. With respect to, say, blockchain, you raised some red flags with respect to privacy about moving more services online. The model that is the foundation of this study is the Estonian model, and I would say that they have three core aspects to that system that help to protect privacy, as far as I understand it.

One is the digital ID, which is an encrypted device that allows for me to access government services and requires additional levels of authentication. Second, they do use blockchain technology. They were using it before the rest of us understood it as blockchain technology. It's KSI Blockchain. It's a particular blockchain technology that they claim was invented in Estonia and is used in over 100 countries around the world. Third, when government employees access people's profiles, it is time-stamped and the purpose and reason for which the government employee accessed that information is transparent.

I guess the real question that I'm driving at is what is the problem with the Estonian model?

● (1615)

Mr. Chris Vickery: The problem with that model is that it only takes one little defect in the armour to ruin the whole thing. Day in and day out for the past few years, I have been hunting down data breaches. I found quite a few and every single company's website that's involved in these data breaches has a statement to the effect that, “We follow industry standard practices”, “we use umpteenth level security and encryption”, etc. I find these databases to be open to the public Internet, not encrypted. They have no password and no user name whatsoever. It only takes one developer to mess things up and cut a corner and do something that is a little too risky and not best practice.

Mr. Nathaniel Erskine-Smith: Just to clarify, if you ever find a way into the system in Estonia, I'd certainly like to know that because if the digital ID is stolen in some way, I understand that they revoke the certificate. I understand they have been operating the system since 2000 and they claim they've never had any identity theft.

If there were to be a significant problem in their system, you would think it would have occurred, since they have been operating it for so long already, but I could be wrong.

Mr. Chris Vickery: Compare that to the claims of the Indian government with the Aadhaar database. They have have made similar claims for that database, yet on several occasions, it's been proven that they have had massive data breaches, both in the access portal and in the basic encoding system of the Aadhaar ID card itself.

I don't know if I believe Estonia when they say they've had no data breaches or problems whatsoever, or if that's just bluff and bluster. Maybe that's something I could look into a little more in-depth.

Mr. Nathaniel Erskine-Smith: If you could, I would appreciate it if you could take some time and look at that with the expertise you have and come back to us with something in writing. That would be very helpful to this committee.

Mr. Carroll, from what you've seen, you have raised concerns about the weaponization of data and the erosion of a shared discourse. Obviously, you've pursued this yourself in a very useful way, in trying to get at this major scandal and really uncover as many answers as you can.

Mr. Kint had referred to some of our recommendations. Have you read our report as well?

Mr. David Carroll: Yes.

Mr. Nathaniel Erskine-Smith: Okay. Is there something we missed?

Mr. David Carroll: I'd like the opportunity to go back and reread the report with that question in mind, but I think I admire the audacity of the report to cross potentially a third rail of how our political parties are supposed to be regulating themselves on these issues. That, in my observation, went further than Information Commissioner Denham's recommendation to put an ethical pause on micro-targeting.

I do appreciate that. I think this is the main question for multiple governments around the world. How does the exemption of political targeting break down the whole system? In the case of Cambridge Analytica, political data was used for commercial purposes, and commercial data was used for political purposes. It's quite difficult—

Mr. Nathaniel Erskine-Smith: It would certainly be illegal here, I think it's fair to say, even under our existing rules.

Let's use an example of a change that we have adopted as a government in Bill C-76 with respect to a database. When there are political ads, they have to be put into a searchable database. We then recommended that it has to be as user-friendly as possible, and really, I would say, designed with journalists in mind so that they can do their job and hold people like me accountable for the ads we put in place during elections. Is that sufficient?

When you talk about a shared discourse and echo chambers, as it were, is that a sufficient answer, do you think?

● (1620)

Mr. David Carroll: It's an important start. The level of transparency required to hold this kind of advertising accountable needs to be maximal, I believe. For example, most Facebook users are not aware that political parties and campaigns upload their voter registration files into Facebook to target them individually, by name. The way you find that in the Facebook interface is very difficult, and it doesn't show that one-to-one level marketing in even Facebook's transparency tool that it launched here in Canada.

I think the maximum amount of disclosure will be beneficial to concerned citizens as well. I think it comes down to that granular level. You should know that you've been targeted as an individual voter for particular messages, rather than the segmentations that they claim. Also, people need to know if they've been assigned to what's called a “lookalike audience” as well. That creates a similar kind of one-to-one targeting without your name being attached to it.

I would advocate for as much disclosure as possible when it comes to political advertising, and maybe advertising in general.

Mr. Nathaniel Erskine-Smith: I'm out of time, but I'll take you up on that. When you read our report a second time, get back to us in writing with anything we've missed.

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

Next up for seven minutes is Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

I'd like to start with you, Mr. Vickery. Certainly, the establishment of digital government in Canada will be very different from Estonia's, given that we have provinces and territories, municipal governments, regional governments and the federal government and there are quite clearly defined lines of authority in terms of who has jurisdiction or not.

Even in the establishment of early forms of limited digital government.... Let's say the Canadian government were to look at only the areas of its jurisdiction in relation to the entire population of the country. One would expect that there would be something of a gold rush by companies looking to be the creators, the administrators or the partners, if you will, in creating such a huge digital operation.

The Canadian Bankers Association, or at least the president of the association, has suggested that banks are the most trusted handlers of personal data. They have two-factor logins and they're more responsible, say, than the Equifaxes or other collectors of data, the data brokers, and certainly more responsible than companies such as Alphabet, Google, Facebook and so forth.

I'm just wondering what sorts of guidelines you would suggest to the Government of Canada if it were to set up digital government. What sorts of companies would you recommend to be on the inside in the creation and the maintenance and guarantor of security?

Mr. Chris Vickery: I think the banking idea is not a bad one. That is a highly regulated industry accustomed to things such as very intense audits, keeping paper trails, and doing everything by the book—hopefully. I think they are definitely a good industry to lean on; however, I would be very, very cautious about how you allow the data to then be used in other ways. I would make very bright lines with whoever you go with to lean on and use their expertise and infrastructure, whatever, indicating what is acceptable and what is not. You can't budge or blur the lines here. This is a bright line, and these are the penalties if you break the line, and then enforce that if it happens.

Hon. Peter Kent: With regard to the Estonian model, where there are silos—depending on the different authority concerned, of education, health, taxes or whatever—the individual chip used to access one's personal information or that can be requested from the individual is siloed. However, you raised concerns about the movement of information between silos and the possible points of penetration through either a deliberate or an accidental process in the creation.

● (1625)

Mr. Chris Vickery: Yes, I would caution against allowing the segmented siloed databases to talk to each other. If you need data, get it from the person the data belongs to, because if the databases can talk to each other, the data doesn't really belong to that individual citizen; they're just an optional gatekeeper at that point.

Hon. Peter Kent: Would you suggest that every silo be administered by the creator of the central program?

Mr. Chris Vickery: I think that if you mix and match administrators, that's basically the same thing as mixing and matching the databases. The administrators are just human, and humans want to eliminate work and make things as simple as possible, so that's where corners get cut.

Hon. Peter Kent: I have a couple of questions for Mr. Carroll and Mr. Kint.

Given the impact of the Facebook-Cambridge Analytica-AggregateIQ scandal and the stories that have come out, we saw people cancelling their Facebook accounts. There is skepticism and fear in some quarters about invasion of privacy through social media. How does one reassure the public that digital service provided by government can be secure and protected and that violation of privacy is unlikely, if not impossible?

Mr. Carroll, you may like to go first.

Mr. David Carroll: I think the reaction to the Cambridge Analytica scandal worldwide shows that we have a visceral response to it. We don't know exactly why it upsets us, but it became a household name around the world overnight. To that specific thing, we understand that there are incentives at play, and the government doesn't have an incentive to profit from data or necessarily to use it for nefarious acts. There isn't the sense that there could be rogue actors abusing a system.

My opinion is that as long as breaches at the government level are protected against, as the sort of worst-case scenario, trust in digital government is much more possible than trust in digital advertising.

Mr. Jason Kint: I would only add that this does speak to the issue of why Facebook needs to be held accountable. There's a study each year from Edelman called the "Trust Barometer", and we saw that institutional trust declined in light of Facebook. Edelman went deeper for the first time and started to unpack what was happening, particularly with the trust in media, which is the part I get most concerned about in my role. The trust in journalism was going up or rebounding, and it was actually the trust in platform itself where the issue was. These platforms are embedded in our lives, and they start to affect trust in other areas, so the question of whether we could trust the media started to be impacted by what was going on with Facebook and the declining trust of that platform.

They just put out their new research three weeks ago, and there was a 30-point gap in trust between social media and traditional media. It worries me when you have a platform that's kind of gone awry and it starts to affect everything.

Hon. Peter Kent: How would government reassure for the same reasons? Would you share the same reasons that Mr. Carroll—

Mr. Jason Kint: I think it's holding Facebook accountable. It forces them to raise the trust in their own product, which can be a very long term issue for them—they might be stuck in this bad cycle—and it raises the trust level in the entire platform.

The Chair: Thank you. You have five seconds.

Hon. Peter Kent: No, I'll come back.

The Chair: We'll come back. We'll have time after.

Next up for seven minutes is Mr. Cullen.

Thank you for coming back and gracing us with your presence again in committee. It's good to have you back.

Mr. Nathan Cullen: You can decide after my round of questioning whether it was a graceful presence, but thank you, Chair.

Thank you to our witnesses for being here.

There's a lot I want to explore, but the time is limited so I'll try to keep it tight and bright and follow the chain of events of, say, the interference or the attempted corruption—or successful corruption—of the U.S. election and the Brexit vote.

You talked about accountability, Mr. Kint, in your last piece. Does the chain start with access, illegal or otherwise, to the databases that parties hold on citizens? Parties collect an enormous amount of information about voters, voting intent and location, potentially income and preferences, and that information, once hacked—because there was not sufficient security there—was then allowed to be weaponized through the social media platforms. You talked, in your last comment, about accountability toward Facebook.

This is a life-threatening event for that company. Trust is important to any company, particularly social media. What has the response been like since that line was proven, the hack of the DNC and the Republicans, the targeted lies that were then spread through that election, and Facebook not being accountable to its users for its security?

● (1630)

Mr. Jason Kint: From our perspective it's been very disappointing. I sent a letter on behalf of our association to Mr. Zuckerberg in November 2016 around the time of the election, asking for what we described as "moonshots", saying that it was that big a problem. They clearly have some of the best engineering minds in the world and enormous resources to solve issues like this.

We've been very disappointed. It's been more of a PR strategy than anything, and it seems as though in the last few months it's shifted even more aggressively toward that.

Mr. Nathan Cullen: Toward PR?

Mr. Jason Kint: Toward PR and criticizing the media and anybody who's trying to hold them accountable.

Mr. Nathan Cullen: Okay, that's what I'm looking for, because every company has a culture and this is this company's description of its culture, of having been exposed in a major way.

Recently this government came out with a strategy to combat fake news in our next election, which is just eight or nine months away. When we got down to the part of the plan that dealt with social media, the words "hope" and "expectations" were there but no requirements of social media platforms.

I don't know if you watched any of that announcement, either Mr. Carroll or Mr. Kint, just in terms of what social media has to step up to do in order to keep Canadians protected from foreign or other interference. Is it enough to just hope and expect groups like Facebook and Google to do the right thing when it comes to protecting data, not allowing fake news to be weaponized, targeting voters, misdirecting their votes, misdirecting their intentions?

Mr. Jason Kint: From my perspective, particularly with Facebook, we're past that, and that's where I'm hopeful that the FTC steps in and enforces the consent decree. It's on probation from seven or eight years ago.

For many of the issues you led your question with, including the way the political parties use the data, we need to go way further upstream to the actual collection and use of the data. That's where it sits with Facebook. I can give you another 10 symptoms of the problem, from bots and ad fraud to users installing ad blocking because they don't even want to see ads. I can give you a whole list of ways it's affecting my world, but those are all symptoms of the problem. Even disinformation is a symptom of a problem, and the problem is the data collection at a pervasive level across the web. That needs to be restricted for companies that have the access to most of the activity that happens.

Mr. Nathan Cullen: Now you're challenging their very business model. That is what they're in the business of—data collection and then the marketing of that data, which is highly valuable. What did you say? It's a $150 billion ad market industry across—

Mr. Jason Kint: Yes, across the U.S. and North America, and 85% of the growth is going to two companies whose business is data collection.

Mr. Nathan Cullen: That's based on data collection.

Mr. Jason Kint: Yes, one of the things that's most challenging, going back to their strategy, is that you'll hear Mr. Zuckerberg and Ms. Sandberg both make the point that this is their business and this is the way it works. If not, everybody is going to have to pay for the product, and 2.3 billion people around the world are going to have to pay for it, including in developing nations.

There are steps that can be taken in between that hold them to a higher bar in which they make a little less money.

Mr. Nathan Cullen: Let's talk about that higher bar.

Mr. Carroll, I don't know if you can comment on this or not. I think this committee made the suggestion that political parties, which also collect a lot of data, should be held to the privacy standards that private companies are held to. That is not the case in the government's new election bill. The Chief Electoral Officer was out yesterday saying he was very disappointed that this was not included.

Do you think it should be included in Canadian law?

Mr. David Carroll: Yes, I think that's a bold but necessary step. I commented on that earlier, that I admire the audacity of taking that position.

One thing that got lost in the story is that it was illegal to create political profiles of Americans, according to U.K. law. There was a big debate over whether psychometrics worked or not, and that was a red herring to the unlawful profiling, according to U.K. law. In many ways it seems that the directors of Cambridge Analytica/SCL misunderstood the jurisdictional question. The higher-order question is: why did this business become internationalized? Why was U.S. voter data processed in another country?

I think the first issue at play here is around how we can keep voter data inside the countries of the voters as an initial way to protect it.

● (1635)

Mr. Nathan Cullen: Do you mean the political parties preventing it from being hacked in the first place?

Mr. David Carroll: Sure. How could a political party even justify hiring a foreign company to work on their campaign? How is that even acceptable?

Mr. Nathan Cullen: This government let a contract to Cambridge Analytica for $100,000. That isn't much money, but we don't know what the intent or purpose of the contract was. Then the scandal broke, and we still don't know.

We're looking for lessons learned—these very difficult, painful lessons learned in the U.S., in the U.K., in France and Germany. We're on the cusp of our next election. What would you suggest is the most important of those painful lessons learned that Canada must pick up now? The election cycle is now. We are turning our minds towards a vote in October. What would you cite as number one?

Mr. David Carroll: Within the given infrastructure that's here, how can campaigns and vendors be scrutinized by citizens, civil society, academia and the government itself? If the business of this political engine feels as if it is being scrutinized, that's the best we can hope for in terms of their being on their best behaviour. But moving forward, there are fundamental changes that need to happen.

The Chair: Thank you, Mr. Cullen. We will have time at the end, I'm sure, to ask all the questions that need to be asked. I presume that, but we have lots to ask.

Next up, for seven minutes, is Mr. Baylis.

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

With these behemoths—Facebook and Google—two things have happened. You mentioned one, Mr. Kint, which is the profit. There's a phenomenal profit, but they get that profit by making use of copyright that does not belong to them. They take a music video they know I'll like, and they show it to me. They'll put an ad beside it, and they'll keep the money; the musician gets nothing. Or they'll take a wonderful photo that was captured by a photographer who could have sold it to newspapers and such before. They'll take it, digitize it, and then someone will look for that photo. The company takes it and profits.

They do it to journalists, to writers, musicians, artists—all types. I'm not searching for any content that Google's made. I'm not interested. Facebook doesn't make any content.

I want to talk about the money, the profit motive, first of all. They've been protected by something called “safe harbour”, which means they can say, “Hey, you wanted to see this. I just showed it to you. I'm clean here.” Here in Canada, for example, many of our media outlets are suffering tremendously. They've lost all their ad revenue as well. It doesn't mean that people aren't reading their newspaper articles. They are reading them, but they're reading them through a Google aggregate or something like that, and again, Google's taking the profit.

Do you see a way for Canada to deal with that? If not Canada alone, should we be working with our allies to say that's enough profiteering off of all these people? That's what's given this phenomenal power.

Mr. Jason Kint: Yes. You have a number of recommendations in your report that will start to address the problem. We've talked a lot about the data piece: limiting their use of data, because that's where the value is coming from. As soon as you put a constraint on that, it restricts that profit.

There are very interesting developments, particularly in Europe, around copyright, and it seems they are moving forward again as of yesterday. I'd study those. They've been through a lot of the difficult balancing between copyright and free speech protection.

Yes, there are opportunities there. In your report, some of the evidence that Tristan Harris and a few others provided looked at ways to hold them liable for when they make recommendations. That is interesting to me, when we start to talk about not just links to the content but then using their AI to present recommendations. We have to actually put some liability on them. The real reason they're making money is that they have no liability for anything, but at the same time they get all the money. When there's a problem, it's not their problem; it's the Internet's problem or it's society's problem.

● (1640)

Mr. Frank Baylis: Chris, do you have any thoughts on that?

Mr. Chris Vickery: An original seed of corruption in this whole problem is the concept of micro-targeting. There is something to be said for having an Internet and index and aggregated sources and all that stuff that is useful for looking things up. We've always had phone books and things of that nature, but typically they were the same for everybody. When I look at the *Mona Lisa*, I don't have a personalized version of it coming to me that I find more attractive compared with the person next me. It is a human experience to experience what everybody else is experiencing.

When you throw in micro-targeting, you up the ante on how much this data is worth and how much you can squeeze out of—

Mr. Frank Baylis: You're talking about their ability to use the data to micro-target.

Let me talk another way about how they collect data.

The minute I buy my iPhone and say, “I agree to the terms of use”, I click it or I go into Google and I've implicitly agreed to do something, which is to spy on me. I don't want Apple spying on me for last year, even though they make the argument that it's necessary. That's not true. It's a lie; it's not necessary. I have had no power to go and negotiate my terms of use.

Would it be a good idea if we were to mandate what they can and can't do in terms of their ability to collect the data? That doesn't mean everybody will follow it, but for people like Google and Facebook, if the penalties are large enough for breaking that law, we could use their terms of use and say, “Whatever you put your terms of use on, this is contractually what you can and can't do for Canadians.”

I'd like to hear from all three of you on that. Maybe we'll start with you, Mr. Carroll.

Mr. David Carroll: It would be really interesting to create incentives for the industry to realign itself towards non-personal data and away from personal data.

Mr. Frank Baylis: I'm talking about the government mandating it. I don't care what you do: you're not allowed to do this, you're not allowed to do that. Whatever you think you're allowed to do.... Right now you're allowed to do anything.

Mr. David Carroll: Certainly. The question is how the government can push the industry away from personal data towards a way to monetize non-personal data. There are ways to achieve similar results without using personal data.

In regard to the copyright question, there hasn't been a lot of talk or brainstorming around how taxation can reincentivize the industries, whether it's taxing personal data and exempting non-personal data, whether it's taxing use to fund through copyrights and funding for journalism. There are different models that could be explored to address these issues together, because it's hard to talk about copyright without also talking about data. It's hard to talk about antitrust without also talking about data. The way these issues collude together is very tricky.

Mr. Frank Baylis: Mr. Kint.

Mr. Jason Kint: I would try to avoid the government mandating this, but there are things we can learn from the GDPR in Europe. It is probably the most-discussed regulation around data right now, and probably the most forward-looking.

There's something in there called purpose limitations, which basically says that if I give you consent to use my data for a certain purpose, you can't use it beyond that. That speaks to a lot of what I commented on in my opening remarks around context and consumer expectations.

It's about using the data in the way the user expects based on the original negotiation or relationship when they started, and then limiting it to that. The way Google makes money is by moving from Gmail to location tracking, etc.

Mr. Frank Baylis: Then take my data out of the phone. They keep it tracked for me for the last year. I don't want them to do that. It's not necessary, and I have no power to negotiate with Apple to stop doing it. Only the government can stop doing it.

Mr. Jason Kint: As far as we understand, Apple is not using that data to also then micro-target ads at you or use it for any other purpose.

Mr. Frank Baylis: Absolutely.

You go to a restaurant and they know where you've been. They ask you how the restaurant was. It's used all the time.

● (1645)

Mr. Jason Kint: That's within the device. We can get deep into the weeds but it's—

Mr. Frank Baylis: It's sold off. If I look up restaurants, for example, and am thinking of going to a particular restaurant, and then I happen to go there, then I get, hey, do you want to write a review of this restaurant? They know through this thing that they've sold to someone else, and combined with where I've searched and where I've been, they have put it together, so for sure they are doing this.

Mr. Jason Kint: Either way, without going into the weeds on who's doing what, I think a higher bar is definitely in order and should be discussed for the companies that see a substantial amount of your activity; I call them service providers. That may mean that they can't use the data for that purpose. It's no different from walking into a store, say Target, and they're going to track your data as part of the store experience. That's probably acceptable and you can choose not to go to Target ever again because you don't like it. But if you walk into Target and then they track you outside of the store, everywhere you go, that's the problem you're speaking of, and that's where there needs to be a higher bar.

The Chair: Thank you, Mr. Baylis.

Next up for five minutes we have Mr. Gourde.

[*Translation*]

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

My question is for all the witnesses.

The digital world we're currently experiencing seems to be the same in Canada, the United States and other countries. In the digital world, reality has gone beyond fiction. Things that we couldn't even imagine in 2015 have become a reality. Major companies such as Facebook, Google or other companies that may emerge in the future don't seem to have any limits when it comes to obtaining and accumulating our personal information and storing the information for many years.

Should limits be imposed on these companies in terms of our personal information and how long they can keep it?

Mr. Carroll, you can answer first.

[*English*]

Mr. David Carroll: The GDPR in the EU and, to a degree, the new California Consumer Privacy Act, which will come into effect in 2020, offer us models for setting limits. One limit that you proposed is a limit on data retention. One interesting part about GDPR is the requirement to disclose the data retention duration at the moment of gaining consent. When you sign up for a service the requirement is, “we will hold your data for six months”, and you are learning that limitation at the moment of signing up and giving consent.

I think we have some good models now to work from to evaluate and to see how these limits are set. The other limits that my colleague Mr. Kint has been referencing—limiting use based on the context of collection and prohibiting uses across contexts—would be also important frameworks to establish. The key here is also enforcement. My experience working with the Information Commissioner's Office as well as the court system in the U.K. shows that enforcement of these limits is where the rubber hits the road.

Mr. Jason Kint: I would confirm that last point.

I saw that you were recommending giving more powers to the privacy commissioner. That's hugely important. I think the powers that the ICO commissioner had came in at the 11th hour. She was fortunate to have those, so I would recommend that. Certainly, GDPR, has real teeth to it, with the 4% fine of global turnover. That makes a difference, and we're starting to see some of that enforcement.

I have a lot of check marks next to your recommendations. There are a lot of really good recommendations. The things I put stars next to are super important things like modernizing the Competition Act and really recognizing that these companies—with which, as Mr. Baylis points out, you don't have a fair deal because they have so much power and so much data that you have to use them, and there are only two different operating systems, let's say, or only one search engine—actually should be evaluated based on the data, as part of the trade-in value. The fact that they're free shouldn't allow them to run away with a monopoly.

● (1650)

[*Translation*]

Mr. Jacques Gourde: Mr. Vickery, the floor is yours.

[*English*]

Mr. Chris Vickery: I'd like to bring up the concept that data doesn't really go away. Companies can claim they've deleted it or say whatever the heck they want, but it has been rolled into other things by then. There are derivatives of it and they probably did keep some backups.

I would focus more on the data becoming stale after a while. Therefore, implement new rules, regulations, laws, to tighten their ability to collect the superfluous amounts of data, and let that other data become stale, old and of no use because it's so old. Don't worry about trying to wrest it out of their hands, because you're never going to.

[*Translation*]

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Madame Fortier, for five minutes.

[*Translation*]

Mrs. Mona Fortier: Thank you, Mr. Chair.

Ladies and gentlemen, I want to go back to the study that we're currently conducting. As part of the study, we want to determine how the digitization of government services will affect the protection of personal information. We've looked at the Estonian model, among other things, and we've heard some of your comments on it.

Are there any other models or initiatives from around the world that we should look at closely for the purposes of our study?

I want to hear from Mr. Carroll first, then I'll move on to the other witnesses.

[*English*]

Mr. David Carroll: One aspect of the Estonian model that is important and valuable is the principle of collecting once. Not requiring citizens to keep inputting their data is the key idea of this unified national identity, and it prevents this problem that citizens in most countries face of constantly giving the same information to multiple different entities. Each time data is supplied, another weak point is created.

Figuring out how to make the supply-once and secure-forever model work logically makes a lot of sense, because it also helps separate identity from other data. Having mechanisms to create de-identification and anonymization built into the structure works well and so on.

The Aadhaar model in India, another national identity system. has come up. I can corroborate what Mr. Vickery said about it. I've had students doing their own research who found these systems to be alarmingly easy to penetrate, at least in India. To have a digital model that does not also have a strong data protection regime on top of it is a risky endeavour. In some ways Estonia might be well-placed, because it has both this digital government and 20 or 30-year tradition of European data protection linked to it.

We also look at China as an extreme in the other direction, where a surveillance industry.... The distinction between private enterprise and the government is completely blurred and the use of surveillance for social control and social coercion is quite alarming. We do look at the new emerging privacy and data models around the world to figure out which places are figuring it out.

[*Translation*]

Mrs. Mona Fortier: Okay.

Mr. Kint, the floor is yours.

[*English*]

Mr. Jason Kint: I'm not a security expert, so I'll turn most of my time over to Chris. I have heard positive reflections on the Estonian model and I have not heard the security concerns. The way it's described, it makes sense, but I haven't heard of any issues. It's most often the example that comes up in a positive light and is starting to be studied. It may just be a test of time to make sure it's the right one, but I'll let Chris weigh in.

[*Translation*]

Mrs. Mona Fortier: Mr. Vickery, the floor is yours.

● (1655)

[*English*]

Mr. Chris Vickery: I believe it's healthiest to assume there has been a breach at all times, to make a system so segmented and resilient that even if there is a breach, you can find it, recover quickly and the damage will be minimal. I don't think you should put all your eggs in one basket. I believe the solution to having people submit the same info over and over again is to minimize the amount of information that is necessary from them. For example, here in the United States, we're not supposed to give out our social security numbers all the time, according to the government, yet every doctor's office asks for that number. Doctors' offices shouldn't be asking for it.

Minimize, optimize, make it streamlined, but I just don't think putting all of your eggs in one basket is a good idea.

The Chair: You have one minute and 30 seconds.

[*Translation*]

Mrs. Mona Fortier: Canada also has the distinction of having more than one level of government, namely, the federal, provincial and municipal levels. However, we're talking about a single model in the case of Estonia. If you have any ideas on how we could deal with the fact that we have three levels of government, let us know. We're considering this issue in our study. I don't think that I have enough speaking time to let you answer that question.

[*English*]

The Chair: Next up, for five minutes, we have Mr. Kent.

Hon. Peter Kent: I'd like to come back first to Mr. Vickery. Canadian government departments—a number of them, any number of them—have been hacked any number of times in the last 10 years, most notably by Chinese operators either contracted by the Chinese government or suspected to have an interest in serving Chinese government interests.

The Government of Estonia, in 2007, weathered a huge cyber-attack by Russia. I'll just quote the Estonian website, which reassures Estonians about the security of their site. It says:

> After Estonia's experience with the 2007 cyber attacks, scalable blockchain technology was developed to ensure integrity of data stored.... Estonia became host to the NATO Cooperative Cyber Defence Centre of Excellence and the European IT agency.

All of that said—and it does seem to be a good system—do you believe their system is impenetrable by those who would hack it, either through the agencies, the various government agencies holding data, or through one of the users, one of the possessors of an identity card and the chip it contains?

Mr. Chris Vickery: Absolutely not. I would not take the assurances in that regard on their own website to be the bare truth. If they're citing something that happened in 2007, that was 12 years ago. Has nobody tried to hack them since? Can they come up with no other examples? Something that happened 12 years ago is the beginning of time, practically, in Internet speak.

Hon. Peter Kent: That said, they seem confident that they haven't been hacked. They acknowledge the attack then, and it's been documented and analyzed—

Mr. Chris Vickery: I guarantee they've been hacked since then. I'll guarantee it. They may not admit it, they may not know about it, but I'll guarantee it's happened.

Hon. Peter Kent: Okay.

Mr. Carroll and Mr. Kint, when the GDPR came into effect last May, a significant number of major mainstream North American news organizations shut down access to their websites by their European subscribers because of the fear that their websites, as they existed, significantly violated some of the new GDPR regulations. To your knowledge—and I ask both of you—through academia or through the marketplace, have any of those companies come to you with requests for advice, guidance, or acknowledging and notifying that they are changing some of their website operations?

Mr. Jason Kint: Not as many sites backed out as you would think based on the press. I think that's very much a talking point that those who don't like GDPR like to use, in particular Google. Tribune Publishing—it was called Tronc at the time—which has a lot of properties underneath it, decided to pull out. That made for a lot of sites. The concern was that 4% turnover of all revenue...and their digital business and probably the number of users they had in Europe was not actually that big as a local newspaper company. It made a decision, which was just a tradeoff of risk versus "Is it worth it?"

The real problem is that the rollout of GDPR, in particular, was troublesome for most publishers. We sent a letter to Google, on behalf of 5,000 publishers here in North America and Europe, because it waited until a month before. It was literally a two-year process. We were trying for a long time to get what its plans were, and then just a month before the GDPR came into effect, it decided to let everybody know what the plans were. It very much wanted to press enforced consent down on the publishers, so that every publisher had to get consent through Google, and then the publishers had to carry that liability as part of it. We sent a letter to Competition Commissioner Vestager in the EU specifically about this issue. It caused a lot of publishers to have to make last-minute decisions.

● (1700)

Hon. Peter Kent: There have been no changes since then?

Mr. Jason Kint: No changes.

Those publishers you referenced who had backed out have not gone back into the market, but I think they likely will. That's a bad outcome, obviously, when the free press isn't available because of regulation.

Hon. Peter Kent: Mr. Carroll.

Mr. David Carroll: I had an opportunity to engage with the industry and the marketplace in many ways prior to GDPR. For example, in 2015, when Apple enabled ad blocking in iOS, that created a considerable discussion in the publishing industry around the effects of this, so I engaged with industry at that time.

What's interesting in looking back on that debate is that it was whether ads were annoying or it was privacy anxiety. I was trying to argue that it was privacy anxiety, and they didn't want to believe me.

Now, after Cambridge Analytica and GDPR, you can make the case that privacy anxiety is a driver in the ad blocking question; therefore, how does it fit into GDPR consent interfaces that explain the business to consumers so they can understand how monetizing works? To me, it's the idea that GDPR was a kind of teachable moment for consumers and the industry, to say that this is how this industry works.

The problem is that the research shows that the more people understand how digital advertising works, the less they like it.

The Chair: Thank you, Mr. Kent.

Next up, for five minutes, Michel.

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

I want to go back to digital services, and I will ask my questions in French.

[*Translation*]

When I buy merchandise at a store, I'm not required to provide my email address or any other information, no matter how confusing it may be for the person at the cash register, who wonders what to do on the machine. I'm able to buy something without providing personal information. I shouldn't need to provide information to buy sports equipment.

However, I believe that when I'm dealing with the government, I'm required to provide personal information. I'll be given a social insurance number if I can at least provide my name and some references. It's the same for my driver's licence. If I don't provide references, I can't obtain a driver's licence or social insurance number. As a result, I can't find legitimate work because the employer needs my social insurance number. I'm required to provide personal information to the government.

In order to provide optimal and more effective service, the government can't help but turn to digital services and the Internet. It must develop techniques, ways and tools to provide more effective service. I'm of the school of thought that no system is 100% secure, simply as a result of the human factor or the possibility of an inside job. These are the worst threats that can't be controlled. Therefore, the government is forced to design a service that will be vulnerable.

How far can it go? How far should it go? Should it consider that, in spite of everything, it must provide digital services?

[*English*]

Mr. Jason Kint: I heard a couple of themes in the question that I think are important observations. One is that the rules of offline content, whether they be what is appropriate or the actual law, haven't properly translated to online content. The same expectations that you would have in a store when you're buying something, you should expect online, which is not asking me for data that isn't necessary—the data minimization that Chris talked about.

I think that's important, and I would stop at that point.

● (1705)

Mr. David Carroll: I think the metaphor Mr. Kint was using for how the online world needs to reflect the expectations and practices of the offline world is really important. We use the metaphor of privacy in the home as an interesting way of thinking about digital privacy. When you invite someone into your house, if it's a stranger, then you might not let them go beyond the entryway. Other people you might let into your kitchen, and other people you might let use your bathroom. Do you let anybody rifle through your bedside table drawer? No. Privacy is a continuum, and I think that continuum needs to be clarified for government services so that when citizens provide identity authentication, they understand it through an off-line-world metaphor.

Of course, government is different from the marketplace. Validating identity as a citizen is different from validating identity as a consumer.

Mr. Michel Picard: Mr. Vickery.

Mr. Chris Vickery: I caution against using too many real-world metaphors to get people to understand the online world. There aren't very many good ones out there. To think about a website as a home or whatever the heck doesn't work for me. Yes, you will have to put government services online. You will have to provide digital government stuff. That's inevitable—unless you want to be a backwoods caveman society, as I'm sure you do not. You have to develop the norms and acceptable practices of the online world. You can't tie it too much to metaphors from the off-line world, because there aren't very many good analogies that fit, piece to piece to piece.

Mr. Michel Picard: Thank you.

The Chair: Thank you.

Before I go to our last questioner on the list, we do have some time, about 20 minutes, so if you still have a question to ask, just signal the chair. We will put your name down and we will go the full time.

You have three minutes, Mr. Johns.

Mr. Gord Johns (Courtenay—Alberni, NDP): Thank you, Mr. Chair.

Thank you for being here today and for your testimony.

As society becomes increasingly digitalized, do you believe that modifications to the Privacy Act or other legislation should be required for political parties to protect the personal information of Canadians?

I'll start with you, Mr. Kint.

Mr. Jason Kint: I referred to putting a lot of check marks next to your recommendations, and around two I have question marks. Frankly, that was one of them. The argument of being able to also reach certain users is also a good one. The limitations, based on your current privacy law, on how it can be used for political speech I think is something I would want to understand more before I actually weighed in with a hard opinion on it.

Mr. Gord Johns: Do you want to add anything, Mr. Carroll?

Mr. David Carroll: Sure. I think the lesson I learned from pursuing my Cambridge Analytica data was the fundamental necessity of the right of access. The right of access needs to be applied horizontally across the entire civil society, in both the marketplace and the government.

As to this idea that any citizen or consumer should be able to ask an entity for his or her data and be confident that it will be disclosed, what other rights do you stack on top of that? In the case of a political party, if you asked a political party to give you your voter profile, the party should be required to disclose that. If the citizen then wants to dispute or delete it, those are reasonable requests.

Mr. Gord Johns: Okay.

In terms of the digital divide, how can we ensure equal access to government services for people who may not have easy access to the Internet or who, like me, live in rural areas with poor broadband connections? Do you have any thoughts on that?

Mr. Kint, perhaps you can lead off.

● (1710)

Mr. Jason Kint: That has always been a concern, particularly for our news members. At least in the United States, it's been an important initiative. Competition is hugely important in what we call MVPD, the telecom space, with protection of the open Internet in particular to make sure that access is available and further investment to make sure it's subsidized in some way to get access to as many as possible. I think we've gone back and forth on this over the last three or four years in U.S. policy.

Mr. Gord Johns: Mr. Carroll.

Mr. David Carroll: I can relate that to my home state of New York. A major telecom cable provider, as a condition of a merger, was supposed to provide broadband services to rural areas in the state of New York, but failed to do so. The state threatened to kick this provider out of the state if they did not comply. It comes down to enforcement. When you give these companies privileges, they need to pay back.

The Chair: Thank you. We have three five-minute rounds here.

We'll start with Mr. Saini, Ms. Vandenbeld, and then Mr. Erskine-Smith to finish.

Go ahead, Mr. Saini.

Mr. Raj Saini: Mr. Carroll, I have a quick question for you.

You brought up the past. I thought we had studied and finished the Cambridge Analytica study. You prompted one question for me. I still have not received an answer.

Facebook claims the data was deleted. Cambridge Analytica has claimed that they were asked to delete the data, and it was deleted. Do we have any confirmation that this data has been deleted?

Mr. David Carroll: We have no confirmation yet that the data has been deleted. The information—

Mr. Raj Saini: We don't yet know whether 50-million Facebook profiles been deleted.

Mr. David Carroll: Correct.

I can say that just last week at the Sundance Film Festival, a documentary on Netflix premiered. I think some members of this committee are in the film, because the DCMS committee is featured prominently. A former employee featured in the film shows evidence that Facebook-like data was still being pitched to clients after they claimed it was deleted.

We're still seeing evidence bubble up that there haven't been truthful statements. That's why it's not over yet.

Mr. Raj Saini: The reason I suggest this is that.... As you know, Cambridge Analytica closed down in London. The corporate entities have disassembled, in one way or another, and have been recreated with the same players, but with different names. Really, those 50-million profiles are still out there, and companies can still harvest that information. Not only that, they can still build on the information they have. Is that true?

Mr. David Carroll: Yes. I have seen concerns dealing with the insolvency proceedings. Mr. Vickery has also shown me forensic evidence that adds to your concerns.

Mr. Raj Saini: Do I have time?

The Chair: You have three minutes.

Mr. Raj Saini: The other question I have is this. We've talked a lot about data breaches. I just want to change the conversation, in a way. I think our outlook has been that we have to prevent data breaches, but I don't think you'll ever be able to prevent a data breach. I don't care what the entity is, whether it's government or private corporations. Private corporations that have immense wealth are still prone to data breaches.

Is it not better for us to think about different ways? Either we can increase the penalties for those people.... Sometimes, these are non-state actors, and they're outside our jurisdiction—I get that, but in many ways, we can increase the penalties, and more importantly, also maybe diversify the information.

Part of the study is the digital government piece. In Estonia, the data is not held in one database. It's held in multiple databases, and there's an X-Road that connects everything. If you penetrate one aspect of that, you are not going to get the complete information.

Is that a different way to be thinking about things? Eventually, whether this year or next year, we're going to have to come up with some solution. Technology cannot be stopped. We cannot stop citizens from utilizing services. We can't go back to paper and pencil. Either we're going to have to manage the problem or figure out how to limit the damage when a problem occurs. What's your thought on that?

● (1715)

Mr. David Carroll: I think that enforcing transparency in the system is a first important step, giving people this right of access that, when they exercise it, will lift the veil off the black box. I mean that beyond just getting your data, but also the confidence values of predictions—what Chris is talking about, the way our data gets put into data models, then applied to other things and all that stuff requiring transparency.

Related to that, liability for data collection would then reduce the amassing and consolidation of it. As we've discussed here, the fact that two companies have amassed such massive profiles gives them their outsized power.

Mr. Raj Saini: I have a final question.

The Chair: You have a minute.

Mr. Raj Saini: This is something that I think people may not completely understand. When government begins to get into the data collection business, it becomes a competitor of the private data collection business. How do we make sure private entities are part of the solution, as opposed to interfering, impugning or trying to minimize the...? Data collection is king, as you know. When the government starts to collect data—data that maybe private companies don't have access to, such as private health records—how do we make sure that the private sector is part of the solution, as opposed to being competitive?

Mr. David Carroll: The incentives are quite different between a private entity that is trying to monetize data and a government entity that is trying to provide services that are not directly linked to the monetization. You pay your taxes, and you get services, as opposed to your data being used to merchandise your attention. There are technical issues that need to be discussed, but it's hard to equate these two different directionalities with each other.

Mr. Raj Saini: There's going to have to be a point where there's a nexus, where the private sector will have to reveal some information to the government, because, if you hold a bank account or you hold some other financial information at an institution, and the government requires you to fill out your tax form, then there has to be some way of connecting pieces from both the public sector and the private sector.

Mr. David Carroll: Yes, it's weird in the United States. The Internal Revenue Service knows all of our transactions and could do our taxes for us; they're just not allowed to. I think there are interesting ways this does play out, yes.

The Chair: Thank you, Mr. Saini.

Next up is Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you for some very good information.

I want to visit this idea of ownership and right of access, building on the idea of government having very different incentives of providing services, not monetizing. On ownership of data, if it's a company or a political party, and you say you'd like this deleted, then it's easy for us to see why they would have to delete your data. If you want to look at your criminal record or your CRA file or something like that, obviously the citizen doesn't have the same kind of right to delete, amend, change or even to see everything that's there. We're looking at a very different kind of circumstance when we're looking at government collecting data. I wanted to put that to you.

Mr. Vickery especially, you were the one who said that the only way you can have ownership of data is if databases are not talking to each other. You also mentioned translating between databases, but government is doing that all the time, or at least that's something that would be proposed if we had this kind of system.

How do you see those kinds of privacy rules, ownership, consent and right of access in the context of digitized government?

I'll start with Mr. Carroll and then Mr. Vickery, if you want to add anything.

Mr. David Carroll: The right of access definitely needs specific exemptions on the government side, but I would also bring up another necessary exemption, which is to protect journalism and journalists. I think there is GDPR to an extent, but the idea is that journalists need to protect sources, and an opponent of a story could reveal a source inadvertently through the subject access request. You have to be very thoughtful about where you carve out these privileges and responsibilities, and they exist in the private sector in certain ways and definitely in the government sector.

I think you can definitely take a default position that transparency is desirable, so it's about where transparency does not work rather than looking for transparency opportunities.

● (1720)

Ms. Anita Vandenbeld: The exemptions, as opposed to the—

Mr. David Carroll: Privileges, yes.

Ms. Anita Vandenbeld: Mr. Vickery?

Mr. Chris Vickery: I recommend a model going forward that basically defines the terms in very strict ways. If something can be accessed without your permission, you are not the gatekeeper to it, you don't own it and you don't control it. If the government has a criminal record of person X, person X does not own that criminal record. It is a record kept about person X, whereas if Walmart has a shopping history of that person, you could make laws saying that the person has to say it's okay for them to collect it and everything. It's a very different beast, and you've got to let people know that the government holds data on you that you do not own and control. It's just not possible.

Ms. Anita Vandenbeld: Thank you.

The Chair: Last up is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Mr. Carroll, you have talked a lot about the right to know or the right of access. As a politician, I will use examples here that may be far afield. In the election, maybe Mr. Zimmer wants to know who owns a gun and maybe I want to know who has a pet, and we're going to be knocking on doors and trying to target people. I think the right to access has a necessary moderating influence, in the sense that I'm going to be less likely to collect a mountain of information if I know that you, as a voter, are going to be able to see what I've collected about you. I'm probably not going to collect information that you're divorced if I have a great Divorce Act amendment because I think it's going to be really good for you. If you're able to access that, then I'm not going to do it. I think that's a really important right as far as it goes. As politicians, I think we should all subject ourselves to that right of citizens.

The right to correct makes a lot of sense to me as well. It's better for me. It's better for you as a voter.

The right to delete.... I don't know if you have turned your minds to other rights as far as it goes. As someone running for office, I can access certain information that is given to me by Elections Canada that isn't given to people who aren't. I don't think that information should be deleted as far as it goes.

With respect to other information, how far should that right to delete go? If I know you are really concerned about the global compact for migration and I don't really want to get you out to vote because I think that's a crazy position to take, should I delete that if you ask me to delete it?

Mr. David Carroll: I don't mean to dodge the question, but I will answer it in a way that relates to what the information commissioner in the U.K. has ruled in relation to her investigation. Inferred data is considered personal data when it is attached to an identity. It's this idea of creating predictions about people and that when you attach them to their voter file, it constitutes personal data.

I think it gets to your question about campaigns that are trying to predict the behaviour of potential voters, and it's based on predictions rather than verifiable, deterministic facts. That could be one boundary that needs to be further negotiated. For example, if I have a gun license, then you have a verifiable fact that I support gun rights. Whereas, if you're using my social media chatter to infer my feelings about gun rights, that's a different threshold that needs to be defined.

Mr. Nathaniel Erskine-Smith: Mr. Kint, you said you had two question marks next to recommendations in our report. What was the other one?

Mr. Jason Kint: I knew that would happen. It was around content moderation. It was this idea that within a certain set period—I think you suggested 24 hours, maybe—it should be possible to eliminate content. I know that's being rolled out in a couple of different counties in Europe. I think it's probably wise to watch and study it.

Mr. Nathaniel Erskine-Smith: In the first recommendation, you have a question mark beside the wording on taking into account engagement for democratic purposes, which, hopefully, answers the concerns you had.

Mr. Jason Kint: Yes.

Mr. Nathaniel Erskine-Smith: Since you like reading Canadian parliamentary studies—

Voices: Oh, oh!

—I would point out that before we got to the Cambridge Analytica scandal, we published a report on our privacy law, PIPEDA. . One of the recommendations we did make addressed this issue of consent for secondary purposes. Our recommendation was to require explicit consent for secondary uses, which I think would address a lot of the concerns you have raised.

● (1725)

Mr. Jason Kint: Absolutely.

Mr. Nathaniel Erskine-Smith: In terms of future lines of study for this committee, the antitrust issues have been raised by a few witnesses, and this idea of ethical AI. I'll finish with something that Mr. Baylis was talking about, which I think touches on both in a way. When I post a music video or whatever on Facebook and Facebook is able to monetize that, it's that monetization—that pushing it into newsfeeds where they have acted now as editor—where it seems to me that safe harbour rules maybe ought not to apply in the same way.

I don't know if you have a view on that.

Mr. Jason Kint: I do. I think that's an interesting point in the recommendations. I think it was in the evidence from Tristan Harris.

The safe harbour has been used widely, including in our safe harbour in the U.S. There has been a lot of press recently around the harms that are happening within recommendations—within YouTube and the AI, which is clearly aligned with profit and designed by humans. There's an issue there.

Mr. Nathaniel Erskine-Smith: I guess the idea is that as algorithms replace editors, we have to hold to account in the same way those who use algorithms for profit.

Mr. Jason Kint: The auditing of algorithms is the concept you have in there, too, which I think is very wise to look at.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: As the chair, I'm just going to ask one question.

Not to be overly simplistic, I see the solution as quite simple. The penalties are one thing that we heard from the information commissioner in the U.K. too, and something that we need to have on this side in limiting data collection, and understanding that data is a multi-level thing, not just data in a general sense.

You have the floor with us. We're listening to exactly what you say. What I'm going to ask all three of you is simply this. If you have one last thing you really want us to hang onto, what would it be? What would you leave us with in regard to what we're talking about today on data collection and government services, or just in general?

We'll start with Mr. Vickery.

Mr. Chris Vickery: I would leave you with a very bleak current outlook on it. Things need to change dramatically.

Right now, things are 10 times worse than you think they are, and we need action. We need less talk and more action.

The Chair: We do have time for this, but what you mean, "worse than we think"? Could you explain that a bit?

Mr. Chris Vickery: Everybody has breach fatigue because they see all of the data breaches in the news and everything. The number of data breaches that get mentioned in articles is abysmally small. The number of data breaches that actually occur and the amount of data being passed around, whether you want to count employees sharing too much or sending to their personal email or something such as that just in the course of business, is 10 times, 100 times larger than anybody on this committee has their head wrapped around. It is horrifying how bad it is out there right now.

The Chair: Thank you, Mr. Vickery.

Mr. Carroll, and then Mr. Kint.

Mr. David Carroll: The United States, Canada and other countries need to adopt some version of the GDPR, some adaptation of what has been put in that model. The California act moves the needle in the United States and there will be an aggressive race before the California act comes into play to pre-empt state law with a national privacy act of some sort.

It's really a key moment for the United States and Canada to lead and, in a sense, catch up with two decades' worth of data protection that our friends across the Atlantic have achieved.

The Chair: Mr. Kint.

Mr. Jason Kint: I absolutely agree that the model of the GDPR is important. However, to add to that, I would really amplify what's in recommendations 12 and 13 regarding the Competition Act and the intersection with data and the value of data. That solves a lot of issues. It solves liability issues; it solves holding large power plays accountable.

If you start there, you intersect with what I consider really the core issue here: the collection of data in order to make money in ways that are well beyond consumer expectations. Then you bring in enforcement on top of that.

I was at a major privacy conference in Brussels last week. I was on Commissioner Denham's panel and there was a lot of discussion about consent and data. I asked an audience of about 300 people to raise their hand if they used a Google product. Everybody raised their hand. Then I said, "Raise your hand if you're okay with Google tracking and collecting data on everything you do", and nobody raised their hand, of course.

Then I looked at Commissioner Denham and I said, "You have an enforcement issue, because 90% of these people have given consent to do something they don't actually want to have happen."

We need to solve that problem and you have an opportunity to lead the international community here by building from what Europe has done.

● (1730)

The Chair: I would finish by thanking all of you for appearing today. I know some of you travelled many miles to get here and I appreciate your trip. Your testimony today is invaluable. Again, thank you for your testimony and for coming to Canada.

Mr. Jason Kint: It's an honour to be here. Thank you.

Mr. David Carroll: It's an honour to be here. Thank you for having us.

The Chair: The meeting is adjourned.